(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年4 月11 日 (11.04.2002)

PCT

(10) 国際公開番号
WO 02/30054 A1

(51) 国際特許分類[7]: H04L 12/28, G06F 13/00

(21) 国際出願番号: PCT/JP01/08034

(22) 国際出願日: 2001 年9 月17 日 (17.09.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-298590 2000 年9 月29 日 (29.09.2000) JP

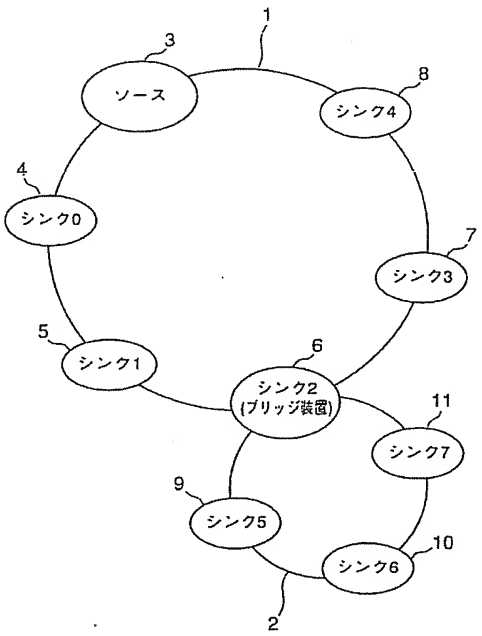
(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 山田正純 (YAMADA, Masazumi) [JP/JP]; 〒543-0071 大阪府大阪市天王寺区生玉町11-14-301 Osaka (JP). 飯塚裕之 (IITSUKA, Hiroyuki) [JP/JP]; 〒576-0033 大阪府交野市私市6-25-6 Osaka (JP). 臼木直司 (USUKI, Naoshi) [JP/JP]; 〒614-8331 京都府八幡市橋本意足26-12 Kyoto (JP).

[続葉有]

(54) Title: COPYRIGHT PROTECTIVE SYSTEM, TRANSMITTER, RECEIVER, BRIDGE DEVICE, COPYRIGHT PROTECTIVE METHOD, MEDIUM, AND PROGRAM

(54) 発明の名称: 著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラム



3...SOURCE
4...SINK 0
5...SINK 1
6...SINK 2 (BRIDGE DEVICE)
7...SINK 3
8...SINK 4
9...SINK 5
10...SINK 6
11...SINK 7

(57) Abstract: If a bridge device is connected to a network such as of a IEEE1394 bus, the desire of the copyright owners to limit the number of devices that can receive a signal cannot be met. A copyright protective system is characterized in that it is connected to a network and comprises one or more receivers for receiving and using data the copyright of which should be protected and a transmitter or transmitting the data the copyright of which should be protected to the receivers through the network, the transmitter (20) includes transmission-side authentication means (23) for authentication together with the receivers and authentication count means (24) for counting the authentications that the transmission-side authentication means (23) has made, and each of the receivers includes reception-side authentication means for authentication together with the transmission-side authentication means so as to limit the authentications.

[続葉有]

WO 02/30054 A1

(74) 代理人: 弁理士　松田正道(MATSUDA, Masamichi); 〒532-0003 大阪府大阪市淀川区宮原5丁目1番3号 新大阪生島ビル Osaka (JP).

(81) 指定国 (国内): JP, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

ＩＥＥＥ１３９４バスなどのネットワークにブリッジ装置が接続されると、信号を受け取られる機器の数を制限したいという著作権者の要望を守ることが出来ない。

ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも１台以上の受信装置と、受信装置に、ネットワークを利用して著作権保護が必要なデータを送信する送信装置２０とを備え、送信装置２０は、受信装置と認証を行う送信側認証手段２３と、送信側認証手段２３が認証した数である認証数を数える認証数カウント手段２４とを有し、受信装置は、送信側認証手段と認証を行う受信側認証手段を有し、前記認証数に制限を設けたことを特徴とする。

明　細　書

著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラム

技術分野

本発明は、著作権保護が必要なデータの著作権を保護してデータを送受信する著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムに関するものである。

背景技術

近年、ＡＶ機器間を接続するネットワークの技術が普及している。このようなネットワークの１つとしてＩＥＥＥ１３９４－１９９５規格（以下ＩＥＥＥ１３９４と呼ぶ）のシリアルバス（以下ＩＥＥＥ１３９４バスと呼ぶ）が存在する。ＩＥＥＥ１３９４は、シリアル伝送を行う高速バスシステムの規格であり、データを同期伝送できるため、ＡＶデータなどのリアルタイム伝送が可能である。このようなＩＥＥＥ１３９４は、家庭用ディジタルＡＶ機器を始め、多くのディジタル映像音声機器に外部用インターフェースとして搭載されようとしている。

一方、新作の映画や有料放送のテレビ番組、音楽などの著作権保護が必要なデータを扱う場合、著作権を保護する必要がある。著作権を保護するための有力な方法として、著作権保護を必要とするデータを暗号化してデータの利用に制限を加える方法がある。

例えば、映像音声データ（以下ＡＶデータと記す）をＩＥＥＥ１３９４バスを利用して伝送する際、ＡＶデータを著作権保護する必要がある場合、そ

のＡＶデータを暗号化して伝送することが行われている。そのような例としてＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）方式が規格化されている。

ＤＴＣＰ方式は、認証機能と鍵の無効化機能を備えており、ＩＥＥＥ１３９４バスでデータ伝送する際に、不正な機器を排除し、ＡＶデータなどの著作権保護が必要なデータを暗号化して伝送することにより著作権の保護を実現している。

コンテンツデータを送信する送信機は、コンテンツデータをコンテンツ鍵で暗号化する。このコンテンツ鍵は送信機により定期的に更新される。更新されるコンテンツ鍵を受信機に安全に渡すため、送信機はコンテンツ鍵を交換鍵と呼ばれる鍵で暗号化して受信機に送信する。

認証機能は暗号化されたデータを解くための鍵をＤＴＣＰのライセンスを受けた受信機にだけ渡すために行われるもので、データに付加されたコピー制限情報（「一回コピー可」「コピー不可」など）と機器の特性（記録機能あり、表示機能のみ、データ内のフォーマット解析・デコードが可能か否かなど）に応じて、公開鍵暗号技術を使用したフル認証と、共通鍵暗号を使用した制限認証を使い分ける。フル認証対応の機器はライセンス機構が付与した署名を含む証明書データを持つ。認証時には、証明書データを送受し、公開鍵暗号技術を使用した電子署名のアルゴリズムを使用して署名が正しいことを判定する。証明書データと併せて乱数を送り合うことにより、認証を行う二台の間でのみ有効な認証鍵を、両方の乱数を用いてそれぞれの機器内で生成できる。

制限認証対応の機器は共通の秘密情報と処理関数を持つ。認証時にはチャレンジ乱数を送信する。乱数を受け取った機器は所定の関数で処理し返送する。チャレンジ乱数を送信した機器は、応答と機器内で処理した値とを比較することにより、正しい機器であることを確認する。認証を行う二台の間で

のみ有効な認証鍵を、両方の乱数を用いてそれぞれの機器内で生成できる。

以上の認証処理により正しい機器であることを確認できると、送信機は、交換鍵を認証鍵で暗号化して受信機に送信する。これにより、受信機側ではコンテンツ鍵を得ることができ、受信したコンテンツの暗号を解いて利用することができる。

以下、図１２を参照して、ＩＥＥＥ１３９４バスシステムについて説明する。

図１２で、ＩＥＥＥ１３９４バス＃１（５０）と、ＩＥＥＥ１３９４バス＃２（５１）はそれぞれ異なったＩＥＥＥ１３９４バスであり、ブリッジ装置５２によって互いに接続されている。

ＩＥＥＥ１３９４バス＃１（５０）には、デバイス＃０（５３）、デバイス＃１（５４）などのデバイスが接続されている。

ＩＥＥＥ１３９４バス＃２（５１）には、デバイス＃０（５８）、デバイス＃１（５９）などのデバイスが接続されている。

デバイス＃０（５３）、デバイス＃１（５４）、デバイス＃０（５８）、デバイス＃１（５９）などは、ＩＥＥＥ１３９４バス＃１（５０）やＩＥＥＥバス＃２（５１）を利用してデータを送信または受信する機器であり、例えばＳＴＢ（セットトップボックス）やＴＶ（テレビ）である。

また、ブリッジ装置５２は、ＩＥＥＥ１３９４バス＃１（５４）に接続されたデバイス＃２（５５）などから送信されたデータを受信して、ＩＥＥＥ１３９４バス＃２に送信する装置である。

ＩＥＥＥ１３９４の規格では、１つのバスに同時に最大６３台までのデバイスを接続することが出来るという制限がある。従って、ＩＥＥＥ１３９４バス＃１（５０）には、同時に最大６３台までのデバイスを接続することが出来、又ＩＥＥＥ１３９４バス＃２（５１）にも、同時に最大６３台までのデバイスを接続することが出来る。

例えば図１２の例では、ＩＥＥＥ１３９４バス＃１（５０）には、ブリッジ装置５２も含めて７台のデバイスが接続されているので、あと５６台接続することが出来る。

デバイス５３は、２０Ｍｂｐｓの伝送レートでデータをアイソクロナス伝送と呼ばれる同期転送によりＩＥＥＥ１３９４バス＃１（５０）の１チャンネルに送信している。そして、デバイス＃１（５４）は、ＩＥＥＥ１３９４バス＃１（５０）の１チャンネルに転送されているデータを受信している。

また、デバイス＃４（５６）は、４０Ｍｂｐｓの伝送レートでデータをＩＥＥＥ１３９４バス＃１（５０）の６３チャンネルに送信している。そして、デバイス＃５（５７）は６３チャンネルで伝送されているデータを受信している。

同様にＩＥＥＥ１３９４バス＃２（５１）では、デバイス＃０（５８）が、２チャンネルに３０Ｍｂｐｓの伝送レートでデータを送信し、２チャンネルに伝送されているデータをデバイス＃１（５９）が受信している。また、デバイス＃３（６１）が３０Ｍｂｐｂのデータを１チャンネルに送信しており、１チャンネルに伝送されているデータをデバイス＃４（６２）と、デバイス＃５（６３）が同時に受信している。

一方、デバイス＃２（５５）は、ＩＥＥＥ１３９４バス＃１（５０）の０チャンネルに２０Ｍｂｐｓの伝送レートでデータを送信している。ブリッジ５２は、ＩＥＥＥ１３９４バス＃１（５０）の０チャンネルに伝送されているデータを受信し、ＩＥＥＥ１３９４バス＃２（５１）の０チャンネルに送信している。そして、デバイス＃２（６０）は、ＩＥＥＥ１３９４バス＃２（５１）の０チャンネルに伝送されているデータを受信している。

このように、アイソクロナス伝送を使用してリアルタイムにデータを伝送することが可能であり、また、２つの異なったＩＥＥＥ１３９４バスをブリッジ装置５２で接続すると、デバイスが送信したデータをブリッジ装置を経

由して異なったバスに接続されたデバイスがリアルタイムに受信することが出来る。

ところで、著作権者からは、著作権保護が必要な映像音声データ（ＡＶデータ）などを送信する際、信号源となる機器からの信号を受けとることが出来る受信機器の数を制限したいという要望がある。

前述したように、１つのＩＥＥＥ１３９４バスには同時に最大６３台しか機器が接続出来ないという制限がある。従って信号源となる機器から送信されたデータを同時に受信出来る受信機器の数は最大でも６２台である。

ところが、上記のように異なったＩＥＥＥ１３９４バスをブリッジ装置で接続すると、信号源となる機器に対してブリッジ装置５２を介した他方のバスで何台の受信機器に信号源となる機器からの信号が受信されるかが、把握出来なくなる。例えば、信号源となる機器に対してブリッジ装置５２を介した他方のバスにさらにブリッジ装置が接続されている場合などが起こりうる。このように、ブリッジ装置５２がＩＥＥＥ１３９４バスに接続されると、非常に多数の受信機器に信号源となる機器から送信された信号が受け取られる危険性がある。また、ＩＥＥＥ1３９４バスに限らず、ＵＳＢなどのネットワークの場合でも同様のことが言える。

すなわち、ＩＥＥＥ１３９４バスなどのネットワークにブリッジ装置が接続されると、非常に多数の受信機器に信号源となる機器から送信された著作権保護が必要な信号が受信される危険性があり、信号を受け取られる機器の数を制限したいという著作権者の要望を守ることが出来ないという課題（第１の課題）がある。

また、ＩＥＥＥ１３９４バスにブリッジ装置が接続されていない場合であっても、著作権者が５台までの受信機器にしか信号を受け取られたくないと希望しても、ＩＥＥＥ１３９４バスに同時に６台以上の受信機器を接続すると、著作権者の要望が守られなくなる。また、このことはＩＥＥＥ１３９４

バスに限らず、ＵＳＢなどのネットワークでも同様のことが言える。

すなわち、著作権者が信号を受け取ることが出来る受信機器の台数を指定して制限したいと要望しても、その要望を守ることが出来ないという課題（第２の課題）がある。

発明の開示

本発明は、上記第１の課題を考慮し、ネットワークにブリッジ装置が接続されていても、著作権保護が必要な信号を受け取ることが出来る受信機器の数を制限したいという著作権者の要望を守ることが出来る著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムを提供することを目的とするものである。

また、本発明は、上記第２の課題を考慮し、著作権保護が必要な信号を受け取ることが出来る受信機器の数を受信機器の台数を指定して制限するという著作権者の要望を守ることが出来る著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムを提供することを目的とするものである。

上述した課題を解決するために、第１の本発明（請求項１に対応）は、ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも１台以上の受信装置と、

前記受信装置に、前記ネットワークを利用して前記著作権保護が必要なデータを送信する送信装置とを備えた著作権保護システムであって、

前記送信装置は、前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記受信装置は、前記送信側認証手段と認証を行う受信側認証手段を有し

前記認証数に制限を設けたことを特徴とする著作権保護システムである。

また、第２の本発明（請求項２に対応）は、前記認証数カウント手段は、前記送信側認証手段が認証を行い成功すると、前記認証数を加算することを特徴とする第１の本発明の著作権保護システムである。

また、第３の本発明（請求項３に対応）は、前記受信装置は、前記送信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度認証要求しないことを特徴とする第２の本発明の著作権保護システムである。

また、第４の本発明（請求項４に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置は、再度認証要求することが出来ることを特徴とする第３の本発明の著作権保護システムである。

また、第５の本発明（請求項５に対応）は、前記送信装置は、前記受信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度前記受信装置から認証要求があってもその認証要求を受け付けないことを特徴とする第２の穂発明の著作権保護システムである。

また、第６の本発明（請求項６に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置は、前記ブリッジ装置から認証要求が行われた場合、その認証要求を受け付けることを特徴とする第５の本発明の著作権保護システムである。

また、第７の本発明（請求項７に対応）は、前記送信装置は、前記受信装置と認証を行い成功した場合、再度前記受信装置と認証を行うが、所定の原因によって前記認証がリセットされない限り、たとえその認証に成功しても前記認証数カウント手段は、前記認証数を加算しないことを特徴とする第２の本発明の著作権保護システムである。

また、第８の本発明（請求項８に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記認証数カウント手段は、再度前記ブリッジ装置と認証を行い成功した場合、前記認証数を加算することを特徴とする第７の本発明の著作権保護システムである。

また、第９の本発明（請求項９に対応）は、前記送信側認証手段は、前記受信装置と認証を行い成功した場合、前記受信装置を特定する情報を登録する登録手段と、

前記受信装置から認証要求が行われると、その認証要求がすでに認証を行い成功した前記受信装置からの認証要求かどうかを登録した前記受信装置を特定する情報を利用して行う重複判定手段とを有することを特徴とする第３～８の本発明のいずれかの著作権保護システムである。

また、第１０の本発明（請求項１０に対応）は、前記認証のリセットは、鍵の更新が行われた時に起こることを特徴とする第３～８の本発明のいずれかの著作権保護システムである。

また、第１１の本発明（請求項１１に対応）は、前記認証のリセットは、交換鍵の更新が行われた時に起こることを特徴とする第３～８の本発明のいずれかの著作権保護システムである。

また、第１２の本発明（請求項１２に対応）は、前記ネットワークを他の

ネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置が前記鍵の更新を行った場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第１０の本発明の著作権保護システムである。

また、第１３の本発明（請求項１３に対応）は、前記認証のリセットは、バスリセットされた際に起こることを特徴とする第３～８の本発明のいずれかの著作権保護システムである。

また、第１４の本発明（請求項１４に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置が接続されている前記ネットワークで、前記バスリセットされた場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第１３の本発明の著作権保護システムである。

また、第１５の本発明（請求項１５に対応）は、前記認証数に制限を設けるとは、前記認証数が所定の値以上になった場合、前記送信側認証手段は、前記受信装置からの認証要求を受け付けないことであることを特徴とする第１の本発明の著作権保護システムである。

また、第１６の本発明（請求項１６に対応）は、前記送信側認証手段と認証を行い成功した前記受信装置が、前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止した場合、前記認証数カウント手段は、前記認証数を減算することを特徴とする第１の本発明の著作権保護システムである。

また、第１７の本発明（請求項１７に対応）は、前記ネットワークを他の

ネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止するとは、前記他のネットワークに接続されているすべての前記受信装置が前記送信装置から送られてくる前記著作権の保護が必要なデータの使用を中止したことであることを特徴とする第１６の本発明の著作権保護システムである。

また、第１８の本発明（請求項１８に対応）は、前記送信装置は、前記送信側認証手段と認証を行い成功した前記受信装置を特定する情報を登録する登録手段を有し、

前記認証数カウント手段が前記認証数を減算した場合、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録を解除することを特徴とする第１６の本発明の著作権保護システムである。

また、第１９の本発明（請求項１９に対応）は、前記送信装置は、前記受信装置が、前記著作権保護が必要なデータの使用を中止したかどうかを調査する調査手段を有することを特徴とする第１６の本発明の著作権保護システムである。

また、第２０の本発明（請求項２０に対応）は、前記著作権保護が必要なデータの使用を中止するとは、前記受信装置が前記ネットワークから切り離されることであり、

前記調査手段は、前記受信装置が前記ネットワークから切り離されたかどうかを定期的に調査することを特徴とする第１９の本発明の著作権保護システムである。

また、第２１の本発明（請求項２１に対応）は、前記調査するとは、前記ネットワークに接続されている前記受信装置の数である接続数を定期的に調

査し、前記接続数が減少した場合、どの前記受信装置が前記ネットワークから切り離されたかをチェックすることであることを特徴とする第２０の本発明の著作権保護システムである。

また、第２２の本発明（請求項２２に対応）は、前記調査手段は、前記受信装置の動作状態及び／または接続プラグのアクティブ状態を調べることによって、前記受信装置が前記著作権保護が必要なデータの使用を中止したかをチェックし、

前記認証数カウント手段は、前記調査手段の調査の結果、前記受信装置が前記著作権保護が必要なデータを使用していないようであれば、前記認証数を減算することを特徴とする第１９の本発明の著作権保護システムである。

また、第２３の本発明（請求項２３に対応）は、前記調査手段は、前記受信装置を特定する情報と、その受信装置の署名とを対応付ける対応表を有し、

前記調査手段は、前記対応表を利用して、前記ネットワークから切り離された前記受信装置が認証済みであったかどうかを判定し、

前記認証数カウント手段は、前記判定結果が、前記ネットワークからきりはなされた前記受信装置が認証済みであったことを示す場合、前記認証数を減算することを特徴とする第２０または２１の本発明の著作権保護システムである。

また、第２４の本発明（請求項２４に対応）は、前記受信側認証手段は、前記受信装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止する場合、前記送信装置に前記認証数を減算するためのデクレメント認証要求を行い、

前記送信側認証手段は、前記受信側認証手段と、前記デクレメント認証を行い、

前記認証数カウント手段は、前記デクレメント認証が成功すると、前記認

証数を減算することを特報とする第１６の本発明の著作権保護システムである。

また、第２５の本発明（請求項２５に対応）は、前記デクレメント認証を行うためのコマンドであるデクレメント認証用コマンドが、前記著作権保護が必要なデータを使用する際の認証を行うためのコマンドである認証コマンドとは別に作成されていることを特徴とする第２４の本発明の著作権保護システムである。

また、第２６の本発明（請求項２６に対応）は、前記著作権保護が必要なデータは暗号化されており、

前記デクレメント認証が成功すると、前記受信装置は、前記著作権保護が必要なデータを解読するための鍵を放棄することを特徴とする第２４または２５の本発明の著作権保護システムである。

また、第２７の本発明（請求項２７に対応）は、前記デクレメント認証は、前記著作権保護が必要なデータを使用するための認証とは、署名、認証方法、演算式の少なくとも１つ以上が異なっていることを特徴とする第２４または２５の本発明の著作権保護システムである。

また、第２８の本発明（請求項２８に対応）は、所定の原因によって認証がリセットされた場合、前記認証数カウント手段は、前記認証数を初期化し、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録をすべて解除することを特徴とする第１８の本発明の著作権保護システムである。

また、第２９の本発明（請求項２９に対応）は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられていることを特徴とする第２の本発明の著作権保護システムである。

また、第３０の本発明（請求項３０に対応）は、前記ブリッジ装置は、前記他のネットワークでは、前記送信装置として扱われ、

前記他のネットワークに接続された前記受信装置から認証要求が行われた場合、

その受信装置と認証を行う前に、前記ネットワークに接続された前記送信装置と認証を行い、その送信装置との認証が成功した場合、前記受信装置と認証を行うことを特徴とする第２９の本発明の著作権保護システムである。

また、第３１の本発明（請求項３１に対応）は、前記ブリッジ装置の前記認証数カウント手段が減算された場合、前記ブリッジ装置は、前記ネットワークに接続された前記送信装置と、前記ネットワークに接続された前記送信装置の前記認証数カウント手段がカウントしている前記認証数を減算させるためのデクレメント認証を行うことを特徴とする第２９の本発明の著作権保護システムである。

また、第３２の本発明（請求項３２に対応）は、前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントすることを特徴とする第２９の本発明の著作権保護システムである。

また、第３３の本発明（請求項３３に対応）は、前記ネットワークに新たに前記送信装置が接続された場合、前記ブリッジ装置は、前記ブリッジ装置の前記認証数カウント手段がカウントしていた前記認証数の回数だけ新たに接続された前記送信装置と認証を行うことを特徴とする第３２の本発明の著作権保護システムである。

また、第３４の本発明（請求項３４に対応）は、前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を有し、

前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を

行い成功した数である前記認証数をカウントし、

前記ブリッジ装置は、前記ネットワークに接続された前記送信装置と認証して成功した数を前記鍵カウンタがカウントしている前記許可の限度数とし、

前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数を減算するためのデクレメント認証要求があった場合、前記ブリッジ装置は前記ネットワークに接続されている前記送信装置とデクレメント認証を行わず、その受信装置とデクレメント認証を行い、

前記デクレメント認証が成功すると、前記ブリッジ装置の前記認証数カウント手段は、前記認証数を減算し、

前記他のネットワークに接続されている前記受信装置から新たに認証要求があった際、

前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より小さい場合には、その受信装置と認証を行い、

前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より小さくない場合には、その受信装置と認証を行う前に前記ネットワークに接続されている前記送信装置と認証を行い、その認証が成功した場合、その受信装置と認証を行うことを特徴とする第３０の本発明の著作権保護システムである。

また、第３５の本発明（請求項３５に対応）は、前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から送られてくるデータを再暗号化して、前記他のネットワークに接続されている前記受信装置に送信し、

前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を

行い成功した数である認証数をカウントし、

前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を有することを特徴とする第２９の本発明の著作権保護システムである。

また、第３６の本発明（請求項３６に対応）は、前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数と前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きい場合、その認証要求を許可することを特徴とする第３５の本発明の著作権保護システムである。

また、第３７の本発明（請求項３７に対応）は、前記鍵カウント手段がカウントしている許可の限度数の上限は予め前記ネットワークに接続されている前記送信装置から与えられていることを特徴とする第３６の本発明の著作権保護システムである。

また、第３８の本発明（請求項３８に対応）は、前記鍵カウント手段がカウントしている許可の限度数の上限は、前記ブリッジ装置が前記ネットワークに接続されている前記送信装置と認証を行うことによって、加算されることを特徴とする第３６の本発明の著作権保護システムである。

また、第３９の本発明（請求項３９に対応）は、前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、その認証要求を拒絶することを特徴とする第３５の本発明の著作権保護システムである。

また、第４０の本発明（請求項４０に対応）は、前記ブリッジ装置は、前

記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に前記許可の限度数を加算するよう依頼することを特徴とする第３５の本発明の著作権保護システムである。

また、第４１の本発明（請求項４１に対応）は、前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に認証要求を行い、前記認証が成功した場合、前記鍵カウント手段は、前記許可の限度数を加算することを特徴とする第３５の本発明の著作権保護システムである。

また、第４２の本発明（請求項４２に対応）は、前記ブリッジ装置は、前記他のネットワークに接続された前記受信装置から認証要求される毎に、前記ネットワークに接続された前記送信装置に前記他のネットワークに接続された前記受信装置のうち認証要求を行っているものの台数を通知することを特徴とする第２９の本発明の著作権保護システムである。

また、第４３の本発明（請求項４３に対応）は、前記ブリッジ装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドには、前記台数を通知するためのフィールドが設けられており、前記ブリッジ装置は、前記フィールドを利用して前記台数の通知を行うことを特徴とする第４２の本発明の著作権保護システムである。

また、第４４の本発明（請求項４４に対応）は、前記ブリッジ装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドは、前記ブリッジ装置の機能を有しない前記ネットワークに接続さ

れた前記受信装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドとは区別されていることを特徴とする第２９の本発明の著作権保護システムである。

また、第４５の本発明（請求項４５に対応）は、前記区別は、前記認証コマンドに添付する署名によって行われることを特徴とする第４４の本発明の著作権保護システムである。

また、第４６の本発明（請求項４６に対応）は、送信装置と認証する受信側認証手段を有し、ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも１台以上の受信装置に対して、前記ネットワークを利用して前記著作権保護が必要なデータを送信する送信装置であって、

前記受信側認証手段と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記認証数に制限を設けたことを特徴とする送信装置である。

また、第４７の本発明（請求項４７に対応）は、ネットワークに接続され、著作権保護が必要なデータを受信して使用する受信装置であって、

前記受信装置と認証を行う送信側認証手段と、前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有する送信装置の前記送信側認証手段と認証する受信側認証手段を備え、

前記認証数に制限を設けたことを特徴とする受信装置である。

また、第４８の本発明（請求項４８に対応）は、前記一方のネットワークに接続された送信装置から送信された著作権保護が必要なデータを前記他のネットワークに接続された受信装置に送信するブリッジ装置であって、

前記受信装置と認証を行うブリッジ装置用送信側認証手段と、

前記送信側認証手段が認証した数であるブリッジ装置用認証数を数えるブリッジ装置用認証数カウント手段と、

前記送信装置と認証を行うブリッジ装置用受信側認証手段とを備え、

前記送信装置は、前記ブリッジ装置または前記ネットワークに接続された前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記受信装置は、前記ブリッジ装置または前記他のネットワークに接続された前記送信装置と認証する受信側認証手段を有し、

前記送信側認証手段が数える前記認証数に制限を設けたことを特徴とするブリッジ装置である。

また、第４９の本発明（請求項４９に対応）は、ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも一台以上の受信装置に、前記ネットワークを利用して送信装置から前記著作権保護が必要なデータを送信する著作権保護方法であって、

前記送信装置は、前記受信装置と認証した数である認証数を数え、

前記認証数に制限を設けたことを特徴とする著作権保護方法である。

また、第５０の本発明（請求項５０に対応）は、第１の本発明の著作権保護システムの、前記受信装置における、前記送信側認証手段と認証を行う受信側認証手段と、

前記送信装置における、前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段との全部または一部としてコンピュータを機能させるためのプログラムを担持した媒体であって、コンピュータにより処理可能である媒体である。

また、第５１の本発明（請求項５１に対応）は、第１の本発明の著作権保護システムの、前記受信装置における、前記送信側認証手段と認証を行う受信側認証手段と、

前記送信装置における、前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段との全部または一部としてコンピュータを機能させるためのプログラムである。

なお、第１の他の発明は、前記認証数カウント手段は、前記送信側認証手段が認証を行い成功すると、前記認証数を加算することを特徴とする第４６の本発明の送信装置である。本発明は、第１の他の発明であってもよい。

また、第２の他の発明は、前記受信装置は、前記送信側認証手段と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度認証要求しないことを特徴とする第４６の本発明の送信装置である。本発明は、第２の他の発明であってもよい。

また、第３の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置は、再度認証要求することが出来ることを特徴とする第２の他の発明の送信装置である。本発明は、第３の他の発明であってもよい。

また、第４の他の発明は、前記送信側認証手段は、前記受信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度前記受信装置から認証要求があってもその認証要求を受け付けないことを特徴とする第１の他の発明の送信装置である。本発明は、第４の他の発明であってもよい。

また、第５の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信側認証手段は、前記ブリッジ装置から認証要求が行われた場合、その認証要求を受け付けることを特徴とする第４の他の発明の送信装置である。本発明は、第５の他の発明であってもよい。

また、第６の他の発明は、前記送信側認証手段は、前記受信装置と認証を行い成功した場合、再度前記受信装置と認証を行うが、所定の原因によって前記認証がリセットされない限り、たとえその認証に成功しても前記認証数カウント手段は、前記認証数を加算しないことを特徴とする第１の他の発明の送信装置である。本発明は第６の他の発明であってもよい。

また、第７の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記認証数カウント手段は、再度前記ブリッジ装置と認証を行い成功した場合、前記認証数を加算することを特徴とする第６の他の発明の送信装置である。本発明は、第７の他の発明であってもよい。

また、第８の他の発明は、前記送信側認証手段は、前記受信装置と認証を行い成功した場合、前記受信装置を特定する情報を登録する登録手段と、

前記受信装置から認証要求が行われると、その認証要求がすでに認証を行い成功した前記受信装置からの認証要求かどうかを登録した前記受信装置を特定する情報を利用して行う重複判定手段とを有することを特徴とする第２～７の他の発明のいずれかの送信装置である。本発明は、第８の他の発明であってもよい。

また、第９の他の発明は、前記認証のリセットは、鍵の更新が行われた時に起こることを特徴とする第２～７の他の発明のいずれかに記載の送信装置である。本発明は、第９の他の発明であってもよい。

また、第１０の他の発明は、前記認証のリセットは、交換鍵の更新が行わ

れた時に起こることを特徴とする第２～７の他の発明のいずれかの送信装置である。本発明は第１０の他の発明であってもよい。

また、第１１の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信側認証手段が前記鍵の更新を行った場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第９の他の発明の送信装置である。本発明は、第１１の他の発明であってもよい。

また、第１２の他の発明は、前記認証のリセットは、バスリセットされた際に起こることを特徴とする第２～７の他の発明のいずれかの送信装置である。本発明は、第１２の他の発明であってもよい。

また、第１３の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

送信装置が接続されている前記ネットワークで、前記バスリセットされた場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第１２の他の発明の送信装置である。本発明は、第１３の他の発明であってもよい。

また、第１４の他の発明は、前記認証数に制限を設けるとは、前記認証数が所定の値以上になった場合、前記送信側認証手段は、前記受信装置からの認証要求を受け付けないことであることを特徴とする第４６の本発明の送信装置である。本発明は、第１４の他の発明であってもよい。

また、第１５の他の発明は、前記送信側認証手段と認証を行い成功した前記受信装置が、送信装置から送られてくる前記著作権保護が必要なデータの

使用を中止した場合、前記認証数カウント手段は、前記認証数を減算することを特徴とする第４６の本発明の送信装置である。本発明は、第１５の他の発明でってもよい。

また、第１６の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置が送信装置から送られてくる前記著作権保護が必要なデータの使用を中止するとは、前記他のネットワークに接続されているすべての前記受信装置が送信装置から送られてくる前記著作権の保護が必要なデータの使用を中止したことであることを特徴とする第１５の他の発明の送信装置である。本発明は、第１６の他の発明であってもよい。

また、第１７の他の発明は、前記送信側認証手段と認証を行い成功した前記受信装置を特定する情報を登録する登録手段を備え、

前記認証数カウント手段が前記認証数を減算した場合、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録を解除することを特徴とする第１５の他の発明の送信装置である。本発明は第１７の他の発明であってもよい。

また、第１８の他の発明は、前記受信装置が、前記著作権保護が必要なデータの使用を中止したかどうかを調査する調査手段を備えたことを特徴とする第１５の他の発明の送信装置である。本発明は、第１８の他の発明であってもよい。

また、第１９の他の発明は、前記著作権保護が必要なデータの使用を中止するとは、前記受信装置が前記ネットワークから切り離されることであり、

前記調査手段は、前記受信装置が前記ネットワークから切り離されたかどうかを定期的に調査することを特徴とする第１８の他の発明の送信装置であ

る。本発明は、第１９の他の発明であってもよい。

また、第２０の他の発明は、前記調査するとは、前記ネットワークに接続されている前記受信装置の数である接続数を定期的に調査し、前記接続数が減少した場合、どの前記受信装置が前記ネットワークから切り離されたかをチェックすることであることを特徴とする第１９の他の発明の送信装置である。本発明は、第２０の他の発明であってもよい。

また、第２１の他の発明は、前記調査手段は、前記受信装置の動作状態及び／または接続プラグのアクティブ状態を調べることによって、前記受信装置が前記著作権保護が必要なデータの使用を中止したかをチェックし、

前記認証数カウント手段は、前記調査手段の調査の結果、前記受信装置が前記著作権保護が必要なデータを使用していないようであれば、前記認証数を減算することを特徴とする第１８の他の発明の送信装置である。本発明は、第２１の他の発明であってもよい。

また、第２２の他の発明は、前記調査手段は、前記受信装置を特定する情報と、その受信装置の署名とを対応付ける対応表を有し、

前記調査手段は、前記対応表を利用して、前記ネットワークから切り離された前記受信装置が認証済みであったかどうかを判定し、

前記認証数カウント手段は、前記判定結果が、前記ネットワークからきりはなされた前記受信装置が認証済みであったことを示す場合、前記認証数を減算することを特徴とする第１９または２０の他の発明の送信装置である。本発明は、第２２の他の発明であってもよい。

また、第２３の他の発明は、前記受信側認証手段は、前記受信装置が送信装置から送られてくる前記著作権保護が必要なデータの使用を中止する場合、前記送信側認証手段に前記認証数を減算するためのデクレメント認証要求を行い、

前記送信側認証手段は、前記受信側認証手段と、前記デクレメント認証を

行い、

前記認証数カウント手段は、前記デクレメント認証が成功すると、前記認証数を減算することを特報とする第１５の他の発明の送信装置である。本発明は、第２３の他の発明であってもよい。

また、第２４の他の発明は、前記デクレメント認証を行うためのコマンドであるデクレメント認証用コマンドが、前記著作権保護が必要なデータを使用する際の認証を行うためのコマンドである認証コマンドとは別に作成されていることを特徴とする第２３の他の発明の送信装置である。本発明は、第２４の他の発明であってもよい。

また、第２５の他の発明は、前記著作権保護が必要なデータは暗号化されており、

前記デクレメント認証が成功すると、前記受信装置は、前記著作権保護が必要なデータを解読するための鍵を放棄することを特徴とする第２３または２４の他の発明の送信装置である。本発明は、第２５の他の発明であってもよい。

また、第２６の他の発明は、前記デクレメント認証は、前記著作権保護が必要なデータを使用するための認証とは、署名、認証方法、演算式の少なくとも１つ以上が異なっていることを特徴とする第２３または２４の他の発明の送信装置である。本発明は、第２６の他の発明であってもよい。

また、第２７の他の発明は、所定の原因によって認証がリセットされた場合、前記認証数カウント手段は、前記認証数を初期化し、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録をすべて解除することを特徴とする第１７の他の発明の送信装置である。本発明は、第２７の他の発明であってもよい。

また、第２８の他の発明は、前記認証数カウント手段は、前記送信側認証手段が認証を行い成功すると、前記認証数を加算することを特徴とする第４

７の本発明の受信装置である。本発明は、第２８の他の発明であってもよい。

また、第２９の他の発明は、前記受信側認証手段は、前記送信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度認証要求しないことを特徴とする第２８の他の発明の受信装置である。本発明は、第２９の他の発明であってもよい。

また、第３０の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記ブリッジ装置は、再度認証要求することが出来ることを特徴とする第２９の他の発明の受信装置である。本発明は、第３０の他の発明であってもよい。

また、第３１の他の発明は、前記送信装置は、前記受信側認証手段と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度前記受信側認証手段から認証要求があってもその認証要求を受け付けないことを特徴とする第２８の他の発明の受信装置である。本発明は、第３１の他の発明であってもよい。

また、第３２の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記送信装置は、前記ブリッジ装置から認証要求が行われた場合、その認証要求を受け付けることを特徴とする第３１の他の発明の受信装置である。本発明は、第３２の他の発明であってもよい。

また、第３３の他の発明は、前記送信装置は、前記受信側認証手段と認証を行い成功した場合、再度前記受信側認証手段と認証を行うが、所定の原因

によって前記認証がリセットされない限り、たとえその認証に成功しても前記認証数カウント手段は、前記認証数を加算しないことを特徴とする第２８の他の発明の受信装置である。本発明は、第３３の他の発明であってもよい。

また、第３４の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記認証数カウント手段は、再度前記ブリッジ装置と認証を行い成功した場合、前記認証数を加算することを特徴とする第３３の他の発明の受信装置である。本発明は、第３４の他の発明であってもよい。

また、第３５の他の発明は、前記送信側認証手段は、前記受信側認証手段と認証を行い成功した場合、前記受信側認証手段を特定する情報を登録する登録手段と、

前記受信側認証手段から認証要求が行われると、その認証要求がすでに認証を行い成功した前記受信側認証手段からの認証要求かどうかを登録した前記受信側認証手段を特定する情報を利用して行う重複判定手段とを有することを特徴とする第２９～３４の他の発明のいずれかの受信装置である。本発明は、第３５の他の発明であってもよい。

また、第３６の他の発明は、前記認証のリセットは、鍵の更新が行われた時に起こることを特徴とする第２９～３４の他の発明のいずれかの受信装置である。本発明は、第３６の他の発明であってもよい。

また、第３７の他の発明は、前記認証のリセットは、交換鍵の更新が行われた時に起こることを特徴とする第２９～３４の他の発明のいずれかの受信装置である。本発明は、第３７の他の発明であってもよい。

また、第３８の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記送信装置が前記鍵の更新を行った場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第３６の他の発明の受信装置である。本発明は、第３８の他の発明であってもよい。

また、第３９の他の発明は、前記認証のリセットは、バスリセットされた際に起こることを特徴とする第２９～３４の他の発明のいずれかの受信装置である。本発明は、第３９の他の発明であってもよい。

また、第４０の他の発明は、前記ネットワークを他のネットワークに接続するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記送信装置が接続されている前記ネットワークで、前記バスリセットされた場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする第３９の他の発明の受信装置である。本発明は、第４０の他の発明であってもよい。

また、第４１の他の発明は、前記認証数に制限を設けるとは、前記認証数が所定の値以上になった場合、前記送信側認証手段は、前記受信側認証手段からの認証要求を受け付けないことであることを特徴とする第４７の本発明の受信装置である。本発明は、第４１の他の発明であってもよい。

また、第４２の他の発明は、前記送信側認証手段と認証を行い成功した前記受信側認証手段が、前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止した場合、前記認証数カウント手段は、前記認証数を減算することを特徴とする第４７の本発明の受信装置である。本発明は、第４２の他の発明であってもよい。

また、第４３の他の発明は、前記ネットワークを他のネットワークに接続

するためのブリッジ装置であり、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、受信装置として扱われ、

前記ブリッジ装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止するとは、前記他のネットワークに接続されているすべての受信装置が前記送信装置から送られてくる前記著作権の保護が必要なデータの使用を中止したことであることを特徴とする第４２の他の発明の受信装置である。本発明は、第４３の他の発明であってもよい。

また、第４４の他の発明は、前記送信装置は、前記送信側認証手段と認証を行い成功した前記受信側認証手段を特定する情報を登録する登録手段を有し、

前記認証数カウント手段が前記認証数を減算した場合、前記登録手段は、前記送信側認証手段と認証を行い成功した前記受信側認証手段を特定する情報の登録を解除することを特徴とする第４２の他の発明の受信装置である。本発明は、第４４の他の発明であってもよい。

また、第４５の他の発明は、前記送信装置は、受信装置が、前記著作権保護が必要なデータの使用を中止したかどうかを調査する調査手段を有することを特徴とする第４２の他の発明の受信装置である。本発明は、第４５の他の発明であってもよい。

また、第４６の他の発明は、前記著作権保護が必要なデータの使用を中止するとは、受信装置が前記ネットワークから切り離されることであり、

前記調査手段は、前記受信装置が前記ネットワークから切り離されたかどうかを定期的に調査することを特徴とする第４５の他の発明の受信装置である。本発明は、第４６の他の発明であってもよい。

また、第４７の他の発明は、前記調査するとは、前記ネットワークに接続されている受信装置の数である接続数を定期的に調査し、前記接続数が減少

した場合、どの受信装置が前記ネットワークから切り離されたかをチェックすることであることを特徴とする第４６の他の発明の受信装置である。本発明は、第４７の他の発明であってもよい。

また、第４８の他の発明は、前記調査手段は、前記受信装置の動作状態及び／または接続プラグのアクティブ状態を調べることによって、受信装置が前記著作権保護が必要なデータの使用を中止したかをチェックし、

前記認証数カウント手段は、前記調査手段の調査の結果、前記受信装置が前記著作権保護が必要なデータを使用していないようであれば、前記認証数を減算することを特徴とする第４５の他の発明の受信装置である。本発明は、第４８の他の発明であってもよい。

また、第４９の他の発明は、前記調査手段は、受信装置を特定する情報と、その受信装置の署名とを対応付ける対応表を有し、

前記調査手段は、前記対応表を利用して、前記ネットワークから切り離された前記受信装置が認証済みであったかどうかを判定し、

前記認証数カウント手段は、前記判定結果が、前記ネットワークからきりはなされた前記受信装置が認証済みであったことを示す場合、前記認証数を減算することを特徴とする第４６または４７の他の発明の受信装置である。本発明は、第４９の他の発明であってもよい。

また、第５０の他の発明は、前記受信側認証手段は、受信装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止する場合、前記送信装置に前記認証数を減算するためのデクレメント認証要求を行い、

前記送信側認証手段は、前記受信側認証手段と、前記デクレメント認証を行い、

前記認証数カウント手段は、前記デクレメント認証が成功すると、前記認証数を減算することを特報とする第４２の他の発明の受信装置である。本発

明は、第５０の他の発明であってもよい。

また、第５１の他の発明は、前記デクレメント認証を行うためのコマンドであるデクレメント認証用コマンドが、前記著作権保護が必要なデータを使用する際の認証を行うためのコマンドである認証コマンドとは別に作成されていることを特徴とする第５０の他の発明の受信装置である。本発明は、第５１の他の発明であってもよい。

また、第５２の他の発明は、前記著作権保護が必要なデータは暗号化されており、

前記デクレメント認証が成功すると、受信装置は、前記著作権保護が必要なデータを解読するための鍵を放棄することを特徴とする第５０または５１の他の発明の受信装置である。本発明は、第５２の他の発明であってもよい。

また、第５３の他の発明は、前記デクレメント認証は、前記著作権保護が必要なデータを使用するための認証とは、署名、認証方法、演算式の少なくとも１つ以上が異なっていることを特徴とする第５０または５１の他の発明の受信装置である。本発明は、第５３の他の発明であってもよい。

また、第５４の他の発明は、所定の原因によって認証がリセットされた場合、前記認証数カウント手段は、前記認証数を初期化し、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録をすべて解除することを特徴とする第４４の他の発明の受信装置。本発明は、第５４の他の発明であってもよい。

また、第５５の他の発明は、前記他のネットワークでは、前記送信装置として扱われ、

前記他のネットワークに接続された前記受信装置から認証要求が行われた場合、

前記ブリッジ装置用送信側認証手段が、その受信装置と認証を行う前に、前記ブリッジ装置用受信側認証手段が、前記ネットワークに接続された前記

送信装置と認証を行い、その送信装置との認証が成功した場合、前記ブリッジ装置用送信側認証手段は、前記受信装置と認証を行うことを特徴とする第４８の本発明のブリッジ装置である。本発明は、第５５の他の発明であってもよい。

また、第５６の他の発明は、前記ブリッジ装置用認証数カウント手段が減算された場合、前記ブリッジ装置用受信側認証手段は、前記ネットワークに接続された前記送信装置と、前記ネットワークに接続された前記送信装置の前記認証数カウント手段がカウントしている前記認証数を減算させるためのデクレメント認証を行うことを特徴とする４８の本発明のブリッジ装置である。本発明は、第５６の他の発明であってもよい。

また、第５７の他の発明は、前記ブリッジ装置用認証数カウント手段は、前記ブリッジ装置用送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントすることを特徴とする第４８の本発明のブリッジ装置である。本発明は、第５７の他の発明であってもよい。

また、第５８の他の発明は、前記ネットワークに新たに前記送信装置が接続された場合、前記ブリッジ装置用受信側認証手段は、前記ブリッジ装置用認証数カウント手段がカウントしていた前記認証数の回数だけ新たに接続された前記送信装置と認証を行うことを特徴とする第５７の他の発明のブリッジ装置。本発明は、第５８の他の発明であってもよい。

また、第５９の他の発明は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を備え、

前記ブリッジ装置用認証数カウント手段は、前記ブリッジ装置用送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である前記認証数をカウントし、

前記ネットワークに接続された前記送信装置と認証して成功した数を前記鍵カウンタがカウントしている前記許可の限度数とし、

前記他のネットワークに接続されている前記受信装置から前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数を減算するためのデクレメント認証要求があった場合、前記ブリッジ装置用受信側認証手段は前記ネットワークに接続されている前記送信装置とデクレメント認証を行わず、前記ブリッジ装置用送信側認証手段がその受信装置とデクレメント認証を行い、

前記デクレメント認証が成功すると、前記ブリッジ装置用認証数カウント手段は、前記認証数を減算し、

前記他のネットワークに接続されている前記受信装置から新たに認証要求があった際、

前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より小さい場合には、前記ブリッジ装置用送信側認証手段は、その受信装置と認証を行い、

前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より小さくない場合には、その受信装置と認証を行う前に前記ブリッジ装置用受信側認証手段が前記ネットワークに接続されている前記送信装置と認証を行い、その認証が成功した場合、前記ブリッジ装置用送信側認証手段がその受信装置と認証を行うことを特徴とする第５５の他の発明のブリッジ装置である。本発明は、第５９の他の発明であってもよい。

また、第６０の他の発明は、前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を備え、

前記ネットワークに接続されている前記送信装置から送られてくるデータを再暗号化して、前記他のネットワークに接続されている前記受信装置に送

信し、

前記ブリッジ装置用認証数カウント手段は、前記ブリッジ装置用送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントする第４８の本発明のブリッジ装置である。本発明は、第６０の他の発明であってもよい。

また、第６１の他の発明は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数と前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より大きい場合、その認証要求を許可することを特徴とする第６０の他の発明のブリッジ装置である。本発明は、第６１の他の発明であってもよい。

また、第６２の他の発明は、前記鍵カウント手段がカウントしている許可の限度数の上限は予め前記ネットワークに接続されている前記送信装置から与えられていることを特徴とする第６１の他の発明のブリッジ装置である。本発明は、第６２の他の発明であってもよい。

また、第６３の他の発明は、前記鍵カウント手段がカウントしている許可の限度数の上限は、前記ブリッジ装置用受信側認証手段が前記ネットワークに接続されている前記送信装置と認証を行うことによって、加算されることを特徴とする第６１の他の発明のブリッジ装置である。本発明は、第６３の他の発明であってもよい。

また、第６４の他の発明は、前記ブリッジ装置用送信側認証手段は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より大きくない場合、その認証要求を拒絶することを特徴とする第６０の他の発明のブリッジ

装置である。本発明は、第６４の他の発明であってもよい。

また、第６５の他の発明は、前記ブリッジ装置用送信側認証手段は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に前記許可の限度数を加算するよう依頼することを特徴とする第６０の他の発明のブリッジ装置である。本発明は、第６５の他の発明であってもよい。

また、第６６の他の発明は、前記ブリッジ装置用送信側認証手段は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置用認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ブリッジ装置用受信側認証手段は、前記ネットワークに接続されている前記送信装置に認証要求を行い、前記認証が成功した場合、前記鍵カウント手段は、前記許可の限度数を加算することを特徴とする第３５の他の発明のブリッジ装置である。本発明は、第６６の他の発明であってもよい。

また、第６７の他の発明は、前記ブリッジ装置用送信側認証手段が前記他のネットワークに接続された前記受信装置から認証要求される毎に、前記ブリッジ装置用受信側認証手段が前記ネットワークに接続された前記送信装置に前記他のネットワークに接続された前記受信装置のうち認証要求を行っているものの台数を通知することを特徴とする第４８の本発明のブリッジ装置である。本発明は、第６７の他の発明であってもよい。

また、第６８の他の発明は、前記ブリッジ装置用受信側認証手段が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドには、前記台数を通知するためのフィールドが設けられており、前記ブリッジ装置用受信側認証手段は、前記フィールドを利用して前記台数の通

知を行うことを特徴とする第６７の他の発明のブリッジ装置である。本発明は、第６８の他の発明であってもよい。

また、第６９の他の発明は、前記ブリッジ装置用受信側認証手段が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドは、前記ブリッジ装置の機能を有しない前記ネットワークに接続された前記受信装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドとは区別されていることを特徴とする第４８の本発明のブリッジ装置である。本発明は、第６９の他の発明であってもよい。

また、第７０の他の発明は、前記区別は、前記認証コマンドに添付する署名によって行われることを特徴とする第６９の他の発明のブリッジ装置である。本発明は、第７０の他の発明であってもよい。

図面の簡単な説明

図１は、本発明の第１～第７の実施の形態における著作権保護システムの構成を示す図である。

図２は、本発明の第１の実施の形態におけるＳＴＢの構成を示す図である。

図３は、本発明の第１、第２、第７、第８の実施の形態におけるＴＶ３０の構成を示す図である。

図４は、本発明の第１の実施の形態における認証数カウント手段がカウントしている認証数とデバイス情報格納手段が格納しているデバイス情報の例を示す図である。

図５は、本発明の第２、第７、第８の実施の形態におけるＳＴＢ４０の構成を示す図である。

図６は、本発明の第２の実施の形態における認証数カウント手段がカウントしている認証数とデバイス情報格納手段が格納しているデバイス情報の例

を示す図である。

図７は、本発明の第３の実施の形態におけるＳＴＢの構成を示す図である。

図８は、本発明の第３及び第４の実施の形態におけるＴＶの構成を示す図である。

図９は、本発明の第４の実施の形態におけるＳＴＢの構成を示す図である。

図１０は、本発明の第５の実施の形態におけるブリッジ装置の構成を示す図である。

図１１は、本発明の第５の実施の形態におけるブリッジ装置の動作を説明するステートマシン図である。

図１２は、従来のバスシステムの構成を示す図である。

符号の説明

１　ＩＥＥＥ１３９４バス＃１

２　ＩＥＥＥ１３９４バス＃２

３　ソース

４　シンク０

５　シンク１

６　シンク２（ブリッジ装置）

７　シンク３

８　シンク４

９　シンク５

２０　ＳＴＢ

２１　送信側Ｄ－Ｉ／Ｆ

２２　暗号化手段

２３　送信側認証手段

２４　認証数カウント手段

２５　認証上限数格納手段

２６　カウント調整・判定手段

２７　デバイス情報格納手段

２８　送信側認証選択手段

２９　送信側認証ルール格納手段

３０　ＴＶ

３１　受信側Ｄ－Ｉ／Ｆ

３２　復号手段

３３　認証要求手段

３４　受信側認証手段

３５　受信側認証選択手段

３６　受信側認証ルール格納手段

発明を実施するための最良の形態

以下に、本発明の実施の形態を図面を参照して説明する。

（第１の実施の形態）

まず、第１の実施の形態について説明する。

図１に、本実施の形態の著作権保護システムを示す。

本実施の形態の著作権保護システムは、ＩＥＥＥ１３９４バス＃１（１）、ＩＥＥＥ１３９４バス＃２（２）がシンク２（ブリッジ装置）（６）によって接続され、ＩＥＥＥ１３９４バス＃１（１）には、ソース３、シンク０（４）などが接続されている。また、ＩＥＥＥ１３９４バス＃２（２）には、シンク５（９）、シンク６（１０）などが接続されている。

ＩＥＥＥ１３９４バス＃１（１）とＩＥＥＥ１３９４バス＃２（２）は、それぞれ異なったＩＥＥＥ１３９４バスである。

ソース３は、ＩＥＥＥ１３０４バス＃１（１）に著作権保護が必要なＡＶデータを送信する機器であり、例えばＳＴＢ（セットトップボックス）である。

シンク０（４）、シンク１（５）、シンク３（９）、シンク４（８）は、ＩＥＥＥ１３９４バス＃１（１）に接続されており、ソース３から送信された著作権保護が必要なＡＶデータを受信して使用する機器であり、例えばＴＶ（テレビ）である。

シンク５（９）、シンク６（１０）、シンク７（１１）は、ＩＥＥＥ１３９４バス＃２（２）に接続されており、ＩＥＥＥ１３９４バス＃２（２）に伝送されている著作権保護が必要なＡＶデータを受信して使用する機器であり、例えばＴＶ（テレビ）である。

ブリッジ装置６は、ソース３から送信された著作権保護が必要なＡＶデータを受信して、再暗号化してから送信する装置である。ブリッジ装置６がＡＶデータの伝送を中継するので、ＩＥＥＥ１３９４バス＃１（１）に接続されたソース３から送信された著作権保護が必要なＡＶデータを、ＩＥＥＥ１３９４バス＃２（２）に接続されたシンク５（９）などが受信することが出来る。

図２に、ソース３の構成を示す。図２では、ソース３をＳＴＢ２０として示した。

ＳＴＢ２０は、送信側Ｄ－Ｉ／Ｆ２１、暗号化手段２２、送信側認証手段２３、認証数カウント手段２４、認証上限数格納手段２５、カウント調整・判定手段２６、デバイス情報格納手段２７から構成される。

送信側Ｄ－Ｉ／Ｆ２１は、著作権保護が必要なＡＶデータをアイソクロナスパケットとしてＩＥＥＥ１３９４バス＃１（１）に送信し、またＩＥＥＥ１３９４バス＃１（１）に接続されている他の機器とアシンクロナスパケットでコマンドなどを送受信するためのデジタルインターフェースである。

暗号化手段２２は、チューナ（図示せず）から受信されたＡＶデータを暗号化する手段である。

送信側認証手段２３は、シンク０（４）、シンク１（５）など、ＩＥＥＥ１３９４バス＃１（１）に接続された機器とＡＶデータを使用するための認証と、ＡＶデータの使用を中止するための認証であるデクレメント認証とを行う手段である。このＡＶデータを使用するための認証（以下、単に認証と言う場合は、ＡＶデータを使用するための認証のことを意味するものとする）と、ＡＶデータの使用を中止するための認証であるデクレメント認証（以下、ＡＶデータの使用を中止するための認証のことをデクレメント認証と呼ぶ）は、異なった認証ルールによって行われる。

認証数カウント手段２４は、送信側認証手段２３が、認証を行い成功した数である認証数を、カウント調整・判定手段２６の判定結果に応じて、数える手段である。

認証上限数格納手段２５は、ＳＴＢ２０が送信する著作権保護が必要なＡＶデータを同時に受信して使用出来る機器の台数の上限を格納する手段である。

デバイス情報格納手段２７は、送信側認証手段２３が認証を行い成功した機器のデバイスＩＤを格納する手段である。ここで、デバイスＩＤとは、予め鍵管理センターから与えられているものであり、機器を特定するための情報である。

カウント調整・判定手段２６は、デバイス情報格納手段２５に格納されているデバイスＩＤを利用して、送信側認証手段２３が認証を行い成功した場合、その認証が同一機器との重複した認証であるかどうか調べることによって、認証数カウント手段２４が数えている認証数をカウントアップするかどうかを判定し、また送信側認証手段２３が後述するデクレメント認証を行い成功した場合、認証数カウント手段２４がカウントしている認証数をカウン

トダウンさせるかどうか判定する手段である。

送信側認証ルール格納手段２９は、送信側認証手段２３が行う認証とデクレメント認証とのそれぞれの認証ルールを格納する手段である。

送信側認証選択手段２８は、送信側認証手段２３が認証を行う際には、その認証ルールを選択し、デクレメント認証を行う際には、そのデクレメント認証用の認証ルールを選択するための手段である。

シンク０（４）、シンク１（５）、シンク３（９）、シンク４（８）はぞれぞれ同様の構成を持つ。図３にＴＶ３０として、一台のシンクの構成を示す。

ＴＶ３０は、受信側Ｄ－Ｉ／Ｆ３１、復号手段３２、認証要求手段３３、受信側認証手段３４、受信側認証選択手段３５、受信側認証ルール格納手段３６から構成される。

受信側認証選択手段３５は、アイソクロナスパケットとしてＩＥＥＥ１３９４バス＃２（２）に送信された著作権保護が必要なＡＶデータを受信し、またＩＥＥＥ１３９４バス＃１（１）に接続されている他の機器とアシンクロナスパケットでコマンドなどを送受信するためのデジタルインターフェースである。

復号手段３２は、受信した著作権保護が必要なＡＶデータの暗号を復号する手段である。復号手段３２で復号され平文になったＡＶデータはデコーダ（図示せず）でデコードされ、モニタ（図示）に表示される。

認証要求手段３３は、認証を行うよう要求するための認証コマンド（以下、認証コマンドと呼ぶ）とデクレメント認証を行うよう要求するデクレメント認証用の認証コマンド（以下、デクレメント認証用コマンドと呼ぶ）をＳＴＢ２０に送信する手段である。認証を行うための認証コマンドとデクレメント認証を行うためのデクレメント用認証コマンドは異なってコマンドが用いられる。

受信側認証手段３４は、ＳＴＢ２０の送信側認証手段２３と認証及びデクレメント認証を行う手段である。

受信側認証選択手段３５は、受信側認証手段３４が認証を行う際には認証のための認証ルールを選択し、受信側認証手段３４がデクレメント認証を行う際には、デクレメント認証用の認証ルールを選択する手段である。

受信側認証ルール格納手段３６は、認証のための認証ルールとデクレメント認証のための認証ルールを格納する手段である。

なお、本実施の形態のＩＥＥＥ１３９４バス＃１（１）、ＩＥＥＥ１３９４バス＃２（２）は本発明のネットワークの例であり、本実施の形態のソース３すなわちＳＴＢ２０は本発明の送信装置の例であり、本実施の形態のシンク１（５）すなわちＴＶ３０は本発明の受信装置の例であり、本実施の形態の送信側認証ルール格納手段２９、送信側認証手段２８、送信側認証手段は、本発明の送信側認証手段の例であり、本実施の形態の認証上限数格納手段２５、認証数カウント手段２４、カウント調整・判定手段２６は本発明の認証数カウント手段の例であり、本実施の形態の受信側認証ルール格納手段３６、受信側認証選択手段３５、受信側認証手段３５は本発明の受信側認証手段の例であり、本実施の形態のカウント調整・判定手段手段２６は本発明の重複判定手段の例でり、本実施の形態のデバイス情報格納手段２７は本発明の登録手段の例であり、本実施の形態の復号手段３２で復号され平文になったＡＶデータはデコーダ（図示せず）でデコードされ、モニタ（図示）に表示されるとは、本発明の著作権保護が必要なデータを使用することの例である。

次に、このような本実施の形態の動作を説明する。

まず、ソース３がＩＥＥＥ１３９４バス＃１に送信した著作権保護が必要なＡＶデータをシンク１（５）が受信して、シンク１（５）のモニタにその映像音声を表示するまでの動作を説明する。

著作権保護が必要なＡＶデータはＭＰＥＧトランスポートストリームであり、ソース３であるＳＴＢ２０の図示していないチューナで受信されたものとする。そして、ソース３であるＳＴＢ２０が送信する著作権保護が必要なＡＶデータは同時に最大３台までの機器しか受信して使用出来ないという制限が設けられているとする。

この制限を示す情報は、放送局でＡＶデータを送信する際にＭＰＥＧトランスポートストリームの内部に埋め込まれる。ＳＴＢ２０は、チューナで受信したＭＰＥＧトランスポートストリームの内部からこの情報を取り出し、認証上限数格納手段２５は、取り出された情報を参照することによって、認証上限数として３を設定する。

ＳＴＢ２０がチューナで受信したＡＶデータをＩＥＥＥ１３９４バス＃１（１）に送信するためには、まず、送信側Ｄ－Ｉ／Ｆ２１は、ＩＥＥＥ１３９４バス＃１（１）のアイソクロナスリソースマネージャに使用する伝送帯域を指定してチャンネル使用権を要求する。そして、アイソクロナスリソースマネージャからチャンネル使用権が与えられたとする。

そうすると、暗号化手段２２は、チューナで受信された著作権保護が必要なＡＶデータを暗号化して、送信側Ｄ－Ｉ／Ｆ２１に出力する。

送信側Ｄ－Ｉ／Ｆ２１は、暗号化されたＡＶデータからそのヘッダにアイソクロナスチャンネルの番号と自らのノードＩＤを付加したアイソクロナスパケットを作成し、作成したアイソクロナスパケットをＩＥＥＥ１３９４バス＃１（１）に送信する。

このようにしてＳＴＢ２０は、著作権保護が必要なＡＶデータをＩＥＥＥ１３９４バス＃１（１）に送信する。

図４に機器が認証要求する毎に、認証数カウント手段２４がカウントしている認証数とデバイス情報格納手段２７が格納しているデバイスＩＤがどのように変化していくかを示す。現時点では、まだＳＴＢ２０は認証要求を受

けておらず、認証数カウント手段２４がカウントている認証数は０であり、デバイス情報格納手段２７には、いずれの機器のデバイスＩＤも格納していない。

一方、シンク１（５）がソース３が送信しているＡＶデータを受信して使用する場合には、まず、ソース３であるＳＴＢ２０に認証要求を行う。

すなわち、シンク１（５）であるＴＶ３０の受信側Ｄ－Ｉ／Ｆ３１は送信されてくるアイソクロナスパケットを受信して、そのヘッダ情報から送信元のノードＩＤを取得する。そして、認証要求手段３０は、認証を要求するための認証コマンドを受信側Ｄ－Ｉ／Ｆ３１に出力する。ＴＶ３０には予め鍵管理センターからデバイスＩＤが割り当てられており、このデバイスＩＤによってＴＶ３０などの各機器を一意に特定することが出来る。そして、認証要求手段３０が出力した認証コマンドには、ＴＶ３０のデバイスＩＤが付加されている。

受信側Ｄ－Ｉ／Ｆ３０は、認証コマンドを受け取ると、認証コマンドから先に取得した送信元のノードＩＤと自らのノードＩＤをヘッダに付加したアシンクロナスパケットを作成し、ＩＥＥＥ１３９４バス＃（１）に送信する。

そして、受信側認証手段３４は、受信側認証選択手段３５に認証のための認証ルールを選択するよう指示し、これを受けて、受信側認証選択手段３５は、受信側認証ルール格納手段３６から認証のための認証コマンドを選択する。

受信側Ｄ－Ｉ／Ｆ３１は、認証コマンドをアシンクロナスパケットとして、ＳＴＢ２０に送信する。

ＳＴＢ２０の送信側Ｄ－Ｉ／Ｆ２１は、ＴＶ３０の受信側Ｄ－Ｉ／Ｆ３１からアシンクロナスパケットとして送られてきた認証コマンドを受信すると、認証コマンドを送信側認証手段２３に出力する。

送信側認証手段２３は、カウント調整・判定手段２６にＴＶ３０のデバイ

スＩＤを通知し、判定を依頼する。

カウント調整・判定手段２６は、送信側認証手段２３からの依頼を受けて、受け取ったデバイスＩＤがすでにデバイス情報格納手段２７に格納されているかどうかを判定する。そして、認証数カウント手段２４がカウントしている認証数と認証上限数格納手段２５に格納されている認証数の上限値を参照し、次のようにしてＴＶ３０からの認証要求を受理するか拒絶するかを判定する。

すなわち、この認証数が認証数の上限値より小さい場合、認証コマンドを受理すべきと判定する。また、この認証数が上限値と等しいかそれ以上の値であっても、受け取ったデバイスＩＤがデバイス情報格納手段２７にすでに格納されている場合には、認証コマンドを受理すべきと判定する。そして、認証数が認証数の上限値と等しいかそれ以上の値であり、かつ受け取ったデバイスＩＤがデバイス情報格納手段２７に格納されていない場合には、ＴＶ３０からの認証コマンドを拒絶すべきと判定する。

送信側認証手段２３は、この判定結果に従って、受信側認証手段３４と認証を行うかどうかを決定する。

例えば、現時点では、認証上限数格納手段２５が格納している上限数は３であり、認証数カウント手段２４がカウントしている認証数が０であるので、認証数の上限より認証数が小さいので、カウント調整・判定手段２６は認証要求を受理すべきと判定し、この判定結果に従って、送信側認証手段２４は、受信側認証手段３４と認証を行う。

すなわち、送信側認証手段２３は、送信側認証選択手段２８に認証ルールを選択するよう指示し、これを受けて、送信側認証選択手段２８は、送信側認証ルール格納手段２９から認証用の認証ルールを選択する。

送信側認証手段２３は、送信側認証選択手段２８が選択した認証のための認証ルールを用い、受信側認証手段３４は、受信側認証選択手段３４が選択

した認証のための認証ルールを用いて互いに認証を行う。

その結果ＴＶ３０が正当な機器であり、認証が成功すると、送信側認証手段２３と受信側認証手段３４は、ＡＶデータを暗号化及び復号するための鍵を交換する。従って、認証が成功すると、ＴＶ３０は、ＳＴＢ２０から送信されているＡＶデータの暗号を入手した鍵で復号して、デコードして、映像音声をモニタに表示して視聴することが出来る。

また、ＴＶ３０が不正な機器であり、認証が失敗した場合には、上記の鍵の交換は行われない。従って、この場合にはＴＶ３０は、ＳＴＢ２０が送信しているＡＶデータの暗号を復号することが出来ないので、ＡＶデータをデコードしたとしても映像音声をモニタに表示して視聴することが出来ない。

このように著作権保護が必要なＡＶデータは暗号化されて伝送され、認証を行うことによって不正な機器を排除することが出来る。

このようにて認証が成功した場合、送信側認証手段２３は、まず認証コマンドに付加されていたＴＶ３０のデバイスＩＤと認証が成功したことをカウント調整・判定手段２６に通知する。

カウント調整・判定手段２６は、認証が成功した通知を受け取ると、デバイス情報格納手段２７が格納しているデバイス情報の中に通知されたＴＶ３０のデバイスＩＤがすでに格納されているかどうかを調べる。

そして、ＴＶ３０のデバイスＩＤがデバイス情報格納手段２７にまだ格納されていない場合には、新たにＴＶ３０のデバイスＩＤをデバイス情報格納手段２７に格納する。

さらに、カウント調整・判定手段２６は、ＴＶ３０のデバイスＩＤがデバイス情報格納手段２７に新規に格納した場合、認証数カウント手段２４にカウントしている認証数を１だけカウントアップするよう指示する。ＴＶ３０のデバイスＩＤがすでにデバイス情報格納手段２７に格納されていた場合には、認証数カウント手段２４にカウントしている認証数をカウントアップす

るよう指示しない。

認証数カウント手段２４は、カウント調整・判定手段２６からの指示に従って、カウントしている認証数を１だけカウントアップする。

従って、認証数カウント手段２４は、同一機器と重複して行われた認証は数えない。

さらに、送信側認証手段２３は、受信側認証手段３４との認証で交換した鍵を暗号化手段２２に渡す。

以後、暗号化手段２２は、送信側認証手段２３から渡された鍵でＡＶデータを暗号化して送信側Ｄ－Ｉ／Ｆ２１に出力する。

一方、受信側認証手段３４は、ＳＴＢ２０との認証が成功した場合、その認証で交換した鍵を復号手段３２に出力する。

これ以後、復号手段３２は、ＳＴＢ２０から送信されてきたＡＶデータを、受信側認証手段３４から受け取った鍵で復号し、復号され平文となったＡＶデータは、図示していないデコーダでデコードされアナログ信号に変換されてモニタに表示される。

このようにて、シンク１（５）であるＴＶ３０は、ソース３であるＳＴＢ２０から送信される著作権保護が必要なＡＶデータを受信してモニタに表示する。

つまり、図４に示すように、シンク１（５）が認証を要求して、ＳＴＢ２０と認証を行った結果、成功すると、認証数カウント手段２４がカウントしている認証数は１になり、デバイス情報格納手段２７にはシンク１（５）のデバイスＩＤが格納される。

以上、ソース３がＩＥＥＥ１３９４バス＃１に送信した著作権保護が必要なＡＶデータをシンク１（５）が受信して、シンク１（５）のモニタにその映像音声を表示するまでの動作を説明した。

上記の動作と同様にして、ソース３がＩＥＥＥ１３９４バス＃１（１）に

送信した著作権保護が必要なＡＶデータをシンク０（３）が受信してそのモニタに映像音声を表示出来たとする。すなわち、シンク０（４）とソース３とが認証した結果、その認証が成功したとする。

すなわち、シンク０（４）とソース３とが認証を行う際、シンク０（４）からの認証要求を、送信側認証手段２３が受信すると、カウント調整・判定手段２６に認証要求を受理すべきかどうかの判定を依頼する。

カウント調整・判定手段２６は、認証数カウント手段２４がカウントしている認証数が１であり、認証上限数格納手段２５に格納されている上限数が３であり、認証数の方が上限数よりまだ小さいので、認証を受理するよう判定する。

そして、送信側認証手段２３はこの判定に従ってシンク０（４）と認証を行う。

認証が成功すると、カウント調整・判定手段２６は、デバイス情報格納手段２７にすでにシンク０（４）のデバイスＩＤが格納されているかどうかを調べる。この時点で、デバイス情報格納手段２７に格納されているデバイスＩＤはシンク１（５）のデバイスＩＤだけであるので、シンク０（４）のデバイスＩＤはまだ格納されていない。従って、認証数カウント手段２４がカウントしている認証数を１カウントアップするよう指示する。

認証数カウント手段２４は、カウント調整・判定手段２６からの指示に従って、認証数を１だけカウントアップする。従って、認証数カウント手段２４がカウントしている認証数は現時点で２となる。

以下、上記と同様にしてシンク０（４）は、ソース３から送信されてくるＡＶデータを復号して、モニタにその映像を表示することが出来るようになる。

すなわち、図４に示すように、シンク０（４）が認証要求を行い、ＳＴＢ２０とシンク０（４）が認証を行い、成功すると、認証数カウント手段２４

がカウントしている認証数は２にカウントアップされ、デバイス情報格納手段２７には、シンク１（５）が追加されて、シンク１（５）とシンク０（４）のデバイスＩＤが格納されることになる。

ここで、シンク３（７）がソース３に認証要求を行い認証が成功したとすると、認証数カウント手段２４がカウントしている認証数は３になり、デバイス情報格納手段２７には、シンク０（４）、シンク１（５）、シンク３（７）のデバイスＩＤが格納されている。

すなわち、この時点でソース３が送信ているＡＶデータをモニタに表示している機器は３台である。

すなわち、図４に示すように、シンク３（７）が認証要求を行い、ＳＴＢ２０とシンク３（７）が認証を行い、成功すると、認証数カウント手段２４がカウントしている認証数は３にカウントアップされ、デバイス情報格納手段２７には、シンク３（７）が追加されて、シンク１（５）とシンク０（４）とシンク３（７）のデバイスＩＤが格納されることになる。

ここで、４台目の機器としてシンク４（８）がソース３に認証要求したとする。カウント調整・判定手段２６は、送信側認証手段２３からシンク４（８）のデバイスＩＤと認証が要求されていることを通知されると、上記と同様にして、認証コマンドを受理するかどうかの判定を行う。この場合、デバイス情報格納手段２７には、シンク０（４）、シンク１（５）、シンク３（７）のデバイスＩＤが登録されており、シンク４（８）のデバイスＩＤは登録されていない。そして、認証数カウント数手段２４がカウントしている認証数は３であり、認証上限数格納手段２５が格納している上限数は３である。

従って、デバイス情報格納手段２７には、シンク４（８）のデバイスＩＤは登録されておらず、しかも認証数と上限数が等しくなっているので、カウント調整・判定手段２６は、シンク４（８）からの認証コマンドを拒絶すべきと判定する。送信側認証手段２３は、この判定に従って、シンク４（８）

からの認証要求を拒絶し、この認証は失敗する。

従って、シンク４（８）は、ソース３から送信されているＡＶデータの暗号を復号することが出来ず、モニタにその映像音声を表示することが出来ない。

すなわち、図４に示すように、シンク４（８）が認証要求を行うと、ＳＴＢ２０はその認証要求を拒絶し、認証数カウント手段２４がカウントしているカウント数もデバイス情報格納手段２７が格納しているデバイスＩＤも変化しない。

また、すでに認証に成功したシンク０（４）などの機器が重複して認証要求した場合、認証数カウント手段２４がカウントしている認証数が上限数より小さくなくても、デバイス情報格納手段２７にすでにシンク０（４）のデバイスＩＤが格納されているので、送信側認証手段２４は認証を行う。そして、認証が成功しても、認証数カウント手段２４は、カウントしている認証数をカウントアップしない。ただし、シンク２（ブリッジ装置）（６）などのブリッジ装置が再度証要求を行った場合は、例外として認証数カウント手段２４はカウントしている認証数をカウントアップする。そして、ブリッジ装置からの認証要求はブリッジ装置でない機器からの認証要求とは、別の形式を持つ。例えば、ブリッジ装置は、鍵管理センターからブリッジ装置でない機器とは異なった署名を与えられる。従って、ソース３は、認証コマンドに添付されている署名から認証要求を行った機器がブリッジ装置であるかどうかを判定することが出来る。

すなわち、図４に示すように、シンク０（４）が再度認証要求を行った場合、認証が行われ、その結果認証が成功した場合、認証数カウント手段２４がカウントしている認証数２４は３のままであり、またデバイス情報格納手段２７が格納しているデバイスＩＤは、シンク１（５）、シンク０（４）、シンク３（７）のままである。

このように、ソース３は、認証数が上限数を越える場合に、まだ認証を行っていないシンクからの認証要求を拒絶する。従って、ソース３が送信しているＡＶデータを受信してモニタにその映像音声を表示出来るシンクの台数は最大でも３台に限定することが出来る。

次に、シンク１（５）が、ソース３から送信されてくるＡＶデータをモニタに表示することを止める場合、シンク１（５）は、デクレメント認証を行うことによってソース３に通知する。以下、この場合の動作を説明する。

シンク１（５）であるＴＶ３０の認証要求手段３３は、ＡＶデータをモニタに表示することをやめることを通知するためにデクレメント認証用コマンドを受信側Ｄ－Ｉ／Ｆ３１に出力する。

このデクレメント用認証コマンドは、ＡＶデータをモニタに表示する際に予め行う認証のための認証コマンドとは、別に設けられている。すなわち、認証コマンドとデクレメント用認証コマンドとは、署名、演算式、認証方法が異なっている。

受信側Ｄ－Ｉ／Ｆ３１は、デクレメント用認証コマンドを上記で説明したのと同様にソース３であるＳＴＢ２０に送信する。

送信側Ｄ－Ｉ／Ｆ２１は、デクレメント用認証コマンドを受信すると、送信側認証手段２３に出力する。

そして、送信側認証手段２３は、送信側認証選択手段２８が選択した送信側デクレメント用認証ルールを使用し、また、受信側認証手段３４は、受信側認証選択手段３５が選択した受信側デクレメント用認証ルールを使用し、デクレメント認証を行う。

そして、デクレメント認証が成功すると、送信側認証手段２３は、カウント調整・判定手段２６にデクレメント認証が成功したことを通知する。

カウント調整判定手段２６は、デバイス情報格納手段２７に格納されているシンク１（５）のデバイスＩＤを削除する。そして、認証数カウント手段

２３にカウントしている認証数を１だけカウントダウンするように指示する。これを受けて認証数カウント手段２４は、カウントしている認証数を１だけカウントダウンする。

一方、ＴＶ３０では、デクレメント認証が成功すると、受信側認証手段３４は、復号手段３２にデクレメント認証が成功したことを通知する。

復号手段３２は、受信側認証手段３４からの通知に従って、ＳＴＢ２０から送信されてくるＡＶデータを復号している鍵を削除する。

デクレメント認証の結果、認証数カウント手段２４がカウントしているカウント数は２になり、上限数である３より小さくなった。また、デバイス情報格納手段２７には、シンク１（５）のデバイスＩＤが削除され、シンク０（４）とシンク（３）の２台のデバイスＩＤが格納されている。

すなわち、図４に示すように、シンク１（５）がデクレメント認証を要求し、デクレメント認証に成功した場合、認証数カウント手段２４がカウントしている認証数は、１だけカウントダウンされて２になり、デバイス情報格納手段２７が格納しているデバイスＩＤからシンク１（５）のデバイスＩＤが削除されて、シンク０（４）、シンク３（７）のデバイスＩＤのみが格納されることになる。

ただし、シンク２（ブリッジ装置）（６）が著作権保護が必要なデータの使用を中止する際にもデクレメント認証を行うが、この場合、第５の実施の形態で説明するように、シンク２（ブリッジ装置）（６）は、複数回ソース３とデクレメント認証を行い、ＩＥＥＥ１３９４バス＃２（２）に接続されているシンク５（９）などの全ての機器が著作権保護が必要なデータをデコードして表示することを中止した場合、デバイス情報格納手段２７に格納されているシンク２（ブリッジ装置）（６）のデバイスＩＤの登録が削除される。すなわち、シンク２（ブリッジ装置）（６）がソース３から著作権保護が必要なデータの使用を中止するとは、ＩＥＥＥ１３９４バス＃２（２）に

接続されているシンク５（９）などの全ての機器がそのデータの使用を中止したことを意味する。

この時点でシンク４（８）などが認証要求を行えば、認証数カウント手段２４がカウントしている認証数がその上限数より小さいので、正当な機器であれば認証が成功する。

すなわち、図４に示すように、シンク４（８）が認証要求すると、認証が行われ、成功する。そして、その結果認証数カウント手段２４がカウントしている認証数は３になり、デバイス情報格納手段２７は、シンク０（４）、シンク３（７）、シンク４（８）のデバイスＩＤが格納されることになる。

このように、すでに認証を行い成功した機器は、ＡＶデータの使用を中止する際に、デクレメント認証を要求し、ＳＴＢ２０は、デクレメント認証用コマンドを受信すると、デクレメント認証を行い、成功すると、デバイス情報格納手段２７は、デクレメント認証を要求した機器のデバイスＩＤを削除し、認証数カウント手段２４は、カウントしている認証数を１だけカウントダウンするので、同時にＡＶデータを使用出来る機器の台数の制限を守りながら、他の機器が新たにＡＶデータを使用することも出来る。また、デクレメント用認証コマンドが認証コマンドとは別に設けられているので、不正な機器がデクレメント認証を悪用することを防止することが出来る。

また、ＩＥＥＥ１３９４バス＃１（１）から、いずれかの機器が取り外された場合や新たに機器がＩＥＥＥ１３９４バス＃１に接続された場合には、バスリセットが行われる。このようにバスリセットが発生すると、認証数カウント手段２４がカウントしている認証数は０に初期化され、また、デバイス情報格納手段２７が格納しているデバイスＩＤはすべて削除される。そして、ＴＶ３０の復号手段３２は、使用していたＡＶデータを復号するための鍵を捨ててしまう。このようにバスリセットが発生した場合には、初期状態からの動作を繰り返す。

なお、本実施の形態では、認証コマンドとデクレメント用認証コマンドとは、署名、演算式、認証方法が異なっているとして説明したがこれに限らない。認証コマンドとデクレメント用認証コマンドとは、少なくとも署名、演算式、認証方法のいずれか１つ以上が異なっていさえすればよい。

さらに、本実施の形態では、ＩＥＥＥ１３９４バス＃（１）に接続されている機器の台数が６台の場合について説明したが、これに限らず、３台、１０台、６３台など要するに、６３台以下の任意の台数が接続されていても構わない。

さらに、本実施の形態では、ソース３は、ブリッジ装置以外のシンク１（５）などの機器と認証を行い成功した後、所定の原因によって認証がリセットされるまでの間に認証が成功したシンク１（５）などの機器と再度認証を行うが、たとえその認証に成功しても、認証数カウント手段２４はカウントしている認証数をカウントアップせず、またソース３は、シンク２（ブリッジ装置６などと認証を行い成功した後、所定の原因によって認証がリセットされるまでの間に認証が成功したシンク２（ブリッジ装置）（６）と再度認証を行い、その認証が成功した場合、認証数カウント手段２４はカウントしている認証数をカウントアップするとして説明したが、これに限らない。ソース３は、ブリッジ装置以外のシンク１（５）などの機器と認証を行い成功した後、所定の原因によって認証がリセットされるまでの間に認証が成功したシンク１（５）などの機器から再度認証要求されると、その認証要求を拒絶する。ただし、ソース３がシンク２（ブリッジ装置）（６）と認証を行い成功した後、所定の原因によって認証がリセットされるまでの間にシンク２（ブリッジ装置）（６）から再度認証要求された場合には、その認証要求を受付る。そして、ソース３がシンク２（ブリッジ装置）（６）との再度の認証に成功した場合、認証数カウント手段２４はカウントしている認証数をカウントアップしても構わない。

（第２の実施の形態）

次に、第２の実施の形態について説明する。

本実施の形態の著作権保護システムを第１の実施の形態と同様に図１に示す。

図５に、本実施の形態のソース３をＳＴＢ４０として示す。第１の実施の形態のＳＴＢ２０との相違点は、ＳＴＢ４０が、カウント調整・判定手段２６の代わりに判定手段４１を備える点である。

判定手段４１は、第１の実施の形態で説明したカウント調整・判定手段２６とは異なり、認証要求が重複した認証かどうかの判定を行わない。

また、シンク０（４）、シンク１（５）などは、第１の実施の形態と異なり、任意に再認証要求を行わない。すなわち、シンク０（４）、シンク１（５）などＩＥＥＥ１３９４バス＃１（１）に接続されている機器は、ソース３が鍵の更新を行うか、またはＩＥＥＥ１３９４バス＃１（１）でバスリセットが発生するまでは、重複した認証要求を行わない。それ以外は第１の実施の形態と同様である。

なお、本実施の形態のソース３すなわちＳＴＢ４０は本発明の送信装置の例であり、本実施の形態の認証上限数格納手段２５、認証数カウント手段２４、判定手段４１は本発明の認証数カウント手段の例である。

次に、このような本実施の形態の動作を第１の実施の形態との相違点を中心に説明する。

第１の実施の形態と同様にソース３としてのＳＴＢ４０の認証上限数格納手段２５には３が格納されているとする。すなわち、ＳＴＢ４０が送信する著作権保護が必要なＡＶデータは同時に最大３台までの機器によりモニタに表示して視聴することが出来る。

まだ、シンク１（５）などいずれの機器からも認証要求を受けていない場合、図６に示すように、ソース３としてのＳＴＢ４０の認証数カウント手段

２４がカウントしている認証数は０であり、デバイス情報格納手段２７は、いずれの機器のデバイスＩＤも格納していない。

ここで、シンク１（５）が認証要求を行うと第１の実施の形態と同様にして、認証が行われ、成功する。その結果、図６に示すように、認証数カウント手段２４がカウントしている認証数は１になり、デバイス情報格納手段２７は、シンク１（５）のデバイスＩＤを格納する。

さらに、シンク０（４）が認証要求を行うと第１の実施の形態と同様にして、認証が行われ、成功する。その結果、図６に示すように、認証数カウント手段２４がカウントしている認証数は２になり、デバイス情報格納手段２７は、シンク１（５）とシンク０（４）のデバイスＩＤを格納する。

さらに、シンク３（７）が認証要求を行うと、第１の実施の形態と同様にして、認証が行われ、成功する。その結果、図６に示すように認証数は３、格納しているデバイスＩＤは、シンク１（５）、シンク０（４）、シンク３（７）になる。

さらに、シンク４（８）が認証要求を行うと、認証上限数格納手段２５が格納している上限数と認証数カウント手段２４がカウントしている認証数が等しいので、第１の実施の形態と同様にして、認証要求が拒絶される。その結果、図６に示すように認証数は３のままであり、格納しているデバイスＩＤは、シンク１（５）、シンク０（４）、シンク３（７）のまま変化しない。

次に、第１の実施の形態では、シンク０（４）が再び認証要求を行ったが、本実施の形態のシンク１（５）としてのＴＶ３０の認証要求手段３３は、再認証要求を任意に行わない。すなわち、ＳＴＢ４０が鍵の更新を行うか、またはＩＥＥＥ１３９４バス＃１（１）でバスリセットが発生することによって認証がリセットされるまでは、重複して認証要求を行わない。

従って、判定手段４１は、認証要求された場合、その認証要求が同一の機器から行われたものかどうかの判定は行わない。

以下、シンク１（５）がデクレメント認証を要求し、その後シンク４（８）が認証要求するが、その動作は図６に示すように、第１の実施の形態と同様であるので説明を省略する。

ただし、シンク２（ブリッジ装置）（６）などのブリッジ装置は、ＳＴＢ４０が鍵の更新を行うか、またはＩＥＥＥ１３９４バス＃１（１）でバスリセットが行われることによって認証がリセットされるまでに、ソース３に再度認証要求することが出来る。そしてシンク２（ブリッジ装置）（６）から再度認証要求され、認証を行い成功した場合、認証数カウント手段２４は、カウントしている認証数をカウントアップする。

ところで、ＳＴＢ４０は、所定の時間が経過する毎にＡＶデータを暗号化する鍵を別の鍵に更新する。このとき認証をリセットする。すなわち、今までＡＶデータを暗号化していた鍵の代わりに別の鍵でＡＶデータを暗号化する。

また、ＳＴＢ４０は、上記のように別の鍵に更新した場合、認証数カウント手段２４がカウントている認証数を０に初期化し、デバイス情報格納手段２７に格納ていたデバイスＩＤも削除する。

すなわち、ＳＴＢ４０は、どの機器とも認証をしていない初期状態と同様の状態に戻る。

そして、ＳＴＢ４０が鍵の更新を行うと、ＴＶ３０の復号手段３２は、ＡＶデータを今までの鍵で復号することが出来なくなってしまう。

そこで、ＴＶ３０の認証要求手段３３は、ＳＴＢ４０が鍵の更新を行ったことを確認してから再度認証要求を行う。

さらに、ＳＴＢ４０とＴＶ３０が認証を行い成功した場合、送信側認証手段２３は、受信側認証手段３４に今回の鍵の更新の次の回に行われる鍵の更新で有効になる鍵をも受信側認証手段３４に渡す。

従って、ＳＴＢ４０が鍵の更新を行った後に、認証要求を行っても、復号

手段３２は、ＳＴＢ４０が鍵の交換を行った際に有効になる鍵をすでに入手済みであるので、ＡＶデータの復号を継続して行うことが出来る。

また、ＩＥＥＥ１３９４バス＃１（１）でバスリセットが発生した場合も、認証がリセットされる。つまり、認証数カウント手段２４がカウントている認証数を０に初期化し、デバイス情報格納手段２７に格納ていたデバイスＩＤも削除する。

すなわち、ＳＴＢ４０は、どの機器とも認証をしていない初期状態と同様の状態に戻る。この場合も、上記と同様にしてＴＶ３０の認証要求手段３３は、ＳＴＢ４０が鍵の更新を行ったことを確認してから再度認証要求を行う。

このように、シンク１（５）などの機器が任意に再認証要求を行わないようにすることによっても第１の実施の形態と同様に同時に著作権保護が必要なＡＶデータをモニタに表示することが出来る機器の台数を制限することが出来る。

（第３の実施の形態）

次に、第３の実施の形態について説明する。

本実施の形態の著作権保護システムを第１の実施の形態と同様に図１に示す。

図７に本実施の形態のソース３をＳＴＢ４２として示す。本実施の形態のＳＴＢ４２は第１の実施の形態のＳＴＢ２０とは異なりデクレメント認証を行わず、その代わりに、ＳＴＢ４２は、シンク１（５）などがＡＶデータをデコードしてモニタに表示することを中止したかどうかを定期的に調査する。すなわち、本実施の形態のＳＴＢ４２は、第１の実施の形態のＳＴＢ２０とは異なり、調査手段４３と対応表格納手段５０を備えており、また、認証ルール格納手段２９及び送信側認証選択手段２８を備えていない。

調査手段４３は、シンク１（５）などがＡＶデータをデコードしてモニタに表示することを中止したかどうかを定期的に調査する手段である。

対応表格納手段５０は、ＩＥＥＥ１３９４規格において機器を一意に特定する情報であるノードユニークＩＤと鍵管理センターから署名の一部として割り当てられた機器を一意に特定する情報であるデバイスＩＤとを対応つける対応表を格納する手段である。

また、図８に本実施の形態のシンク１（５）などをＴＶ４４として示す。

本実施の形態のＴＶ４４は、第１の実施の形態のＴＶ３０とは異なり、ＡＶデータをデコードしてモニタに表示することを中止する場合、デクレメント認証を要求しない。すなわち、ＴＶ４４は、受信側認証ルール格納手段３６及び受信側認証選択手段３５を備えていない。

それ以外は、第１の実施の形態と同様である。

なお、本実施の形態のソース３すなわち、ＳＴＢ４２は本発明の送信装置の例であり、本実施の形態のシンク１（５）すなわちＴＶ４４は本発明の受信装置の例であり、調査手段４３、本実施の形態のカウント調整判定・手段２６、対応表格納手段５０、デバイス情報格納手段２７は本発明の調査手段の例である。

次にこのような本実施の形態の動作を第１の実施の形態との相違点を中心に説明する。

図４に示すように、第１の実施の形態と同様にして、シンク１（５）、シンク０（４）、シンク３（７）、シンク０（４）までがこの順に認証要求を行った結果、ソース３としての認証数カウント手段２４がカウントしている認証数が３であり、デバイス情報格納手段２７が、シンク１（５）、シンク０（４）、シンク３（７）のデバイスＩＤを格納しているとする。ただし、ＳＴＢ４２は送信側認証選択手段２９及び送信側認証ルール格納手段２８を備えていないので、ＴＶ４４と認証を行う際、認証ルールの選択は行わない。同様にＴＶ４４も、認証ルールの選択は行わない。

シンク１（５）としてＴＶ４４がソース３としてのＳＴＢ４２から送信さ

れてくるＡＶデータの映像音声をモニタに表示しているものとする。

調査手段４３は、定期的に、シンク０（４）、シンク１（５）などＩＥＥＥ１３９４バス＃１（１）に接続されている機器毎のプラグの状態を調べている。

ここで、プラグとは、ＩＥＥＥ１３９４バスを用いて、ＡＶ機器のデータを伝送したり、機器制御を行うための規格であるＩＥＣ６１８８３で規格化されているものであり、ＩＥＥＥ1.３９４バスに接続された機器間の論理的な接続を管理するための概念である。以下、簡単にプラグについて説明する。

プラグには入力プラグと出力プラグの２種類がある。すなわち、機器がＩＥＥＥ１３９４バスからＡＶデータを入力する機能を持っている場合、その機器は、同時に入力出来るＡＶデータの数つまり同時に入力出来るアイソクロナスチャンネルチャンネルの数と同じ数の入力プラグを持っており、機器がＡＶデータをＩＥＥＥ１３９４バスに出力する機能を持っている場合、その機器は、同時に出力出来るＡＶデータの数つまり同時に出力出来るアイソクロナスチャンネルの数と同じ出力プラグを持っている。

そして、各機器は、一つの入力プラグに対応して、入力プラグの状態を保持するための一つのｉＰＣＲ（入力プラグコントロールレジスタ）を持っている。また、一つの出力プラグに対応して、出力プラグの状態を保持するための一つのｏＰＣＲ（出力プラグコントロールレジスタ）を持っている。

ＩＥＥＥ１３９４バスに接続された機器どうしがＡＶデータの送受信を行う場合には、その機器同士がコネクションを張る必要がある。すなわち、送信側の機器のｏＰＣＲと出力側の機器のｉＰＣＲにコネクションの種類（ブロードキャストコネクションまたはポイントツーポイントコネクション）や、コネクションの数や使用するチャンネル番号などｉＰＣＲとｏＰＣＲに必要な情報を設定することによって、コネクションを張る。また、ＩＥＥＥ１３９４バスに接続された機器がＡＶデータを受信し、デコードして表示する

ことを中止する際には、上記のコネクションを切断する必要がある。この際、ｉＰＣＲやｏＰＣＲに設定されているコネクションの数を減算したり、登録されているコネクションの種類を解除したりすることによって、コネクションを切断する。従って、ｉＰＣＲに設定されている状態を調べることによって、ＡＶデータを機器が受信してデコード表示しているか、ＡＶデータをデコード表示することを中止しているかを知ることが出来る。以上プラグについて説明した。

さて、シンク１（５）が、ソース３から送信されてくるＡＶデータを受信して、デコード表示することを中止したとする。そうすると、そのＡＶデータに対応するｉＰＣＲのコネクションの設定が解除される。

調査手段４３は、シンク１（５）のｉＰＣＲの状態を調べた結果、シンク１（５）がソース３とのコネクションを切断したことがわかったとする。

そうすると、調査手段４３は、シンク１（５）のノードユニークＩＤを取得し、カウント調整・判定手段２６にシンク１（５）のノードユニークＩＤとシンク１（５）がソース３としてのＳＴＢ４２とのコネクションを切断したことを通知する。

カウント調整・判定手段２６は、調査手段４３から通知されると、受け取ったノードユニークＩＤから、対応表格納手段５０に格納されている対応表を利用して、ノードユニークＩＤに対応するシンク１（５）のデバイスＩＤを調べる。

上述したように、図４に示すようにソース３としての認証数カウント手段２４がカウントしている認証数が３であり、デバイス情報格納手段２７が、シンク１（５）、シンク０（４）、シンク３（７）のデバイスＩＤを格納している。

従って、カウント調整・判定手段２６は、シンク１（５）のデバイスＩＤがすでにデバイス情報格納手段２７に格納されているので、デバイス情報格

納手段２７からシンク１（５）のデバイスＩＤを削除し、また認証数カウント手段２４がカウントしている認証数を１だけカウントダウンするよう指示する。これを受けて認証数カウント手段２４は、カウントしている認証数を１だけカウントダウンする。

このように、第１の実施の形態とは異なり、ソース３から送信されているＡＶデータを受信して、デコード表示することを中止した機器を、ソース３であるＳＴＢ４２の調査手段４３が調査することによって、デクレメント認証をしなくても第１の実施の形態と同等の効果を得ることが出来る。

なお、本実施の形態では、調査手段４３は、シンク１（５）などのプラグの状態を調べることによって、シンク１（５）などがＡＶデータを受信してデコード表示することを中止したかどうかを調べるとして説明したが、これに限らない。以下に説明するようにしても構わない。

すなわち、調査手段４３は、各機器のプラグの状態を調べる前に、ＩＥＥＥ１３９４バス＃１（１）に接続されている機器の台数を調べ、この機器の台数が減少した時のみ、どの機器がＩＥＥＥ１３９４バス＃１から取り外されたかを調べ、ＩＥＥＥ１３９４バス＃１から取り外された機器のノードユニークＩＤを取得し、カウント調整・判定手段２６にその機器のノードユニークＩＤと機器がとりはずされたことを通知する。そして、カウント調整・判定手段２６は、通知されたノードユニークＩＤに対応するデバイスＩＤを対応表から求める。そしてカウント調整・判定手段３６は、デバイス情報格納手段２７にその求めたデバイスＩＤが既に登録済みであるかどうか調べる。登録済みである場合は、ＳＴＢ４２と認証済みの機器が取り外されたことになるので、カウント調整・判定手段２６は、認証数カウント手段２４がカウントしている認証数をカウントダウンするよう指示する。この指示を受けて認証数カウント手段２４は、カウントしている認証数をカウントダウンする。さらに、カウント調整・判定手段２６は、デバイス情報格納手段２７に格納

されている取り外された機器のデバイスＩＤを削除する。

ただし、ここでＩＥＥＥ１３９４バス＃１から取り外されるとは、ＩＥＥＥ１３９４バス＃１（１）に接続するコネクタをＩＥＥＥ１３９４バス＃１（１）から取り外したことではなく、ＴＶ４４が受信側Ｄ－Ｉ／Ｆ３１とは別の系統から送られてくるデータを受信し、モニタに表示するようになったことを意味する。

（第４の実施の形態）

次に、第４の実施の形態について説明する。

本実施の形態の著作権保護システムを第１の実施の形態と同様に図１に示す。

図９に、本実施の形態のソース３をＳＴＢ４５として示す。本実施の形態のＳＴＢ４５は第２の実施の形態のＳＴＢ４０とは異なりデクレメント認証を行わず、その代わりに、シンク１（５）などがＡＶデータをデコードしてモニタに表示することを中止したかどうかを定期的に調査する。すなわち、本実施の形態のＳＴＢ４２は、第２の実施の形態のＳＴＢ４０とは異なり、調査手段４３と対応表格納手段５０を備えており、また、認証ルール格納手段２９及び送信側認証選択手段２８を備えていない。

調査手段４３は、シンク１（５）などがＡＶデータをデコードしてモニタに表示することを中止したかどうかを定期的に調査する手段である。

対応表格納手段５０は、ＩＥＥＥ１３９４規格において機器を一意に特定する情報であるノードユニークＩＤと鍵管理センターから割り当てられた機器を一意に特定する情報であるデバイスＩＤとを対応つける対応表を格納する手段である。

また、図８に本実施の形態のシンク１（５）などをＴＶ４４として示す。ＴＶ４４は第３の実施の形態と同様である。

すなわち、本実施の形態のＴＶ４４は、第１の実施の形態のＴＶ３０とは

異なり、ＡＶデータをデコードしてモニタに表示することを中止する場合、デクレメント認証を要求しない。

それ以外は、第２の実施の形態と同様である。

なお、本実施の形態のソース３すなわちＳＴＢ４５は本発明の送信装置の例であり、本実施の形態の対応表格納手段５０、判定手段４１、調査手段４３、デバイス情報格納手段２７は本発明の調査手段の例である。

次にこのような本実施の形態の動作を第２の実施の形態との相違点を中心に説明する。

図６に示すように、第２の実施の形態と同様にして、シンク１（５）、シンク０（４）、シンク３（７）、シンク４（８）までがこの順に認証要求を行った結果、ソース３としての認証数カウント手段２４がカウントしている認証数が３であり、デバイス情報格納手段２７が、シンク１（５）、シンク０（４）、シンク３（７）のデバイスＩＤを格納しているとする。ただし、ＳＴＢ４５は送信側認証選択手段２９及び送信側認証ルール格納手段２８を備えていないので、ＴＶ４４と認証を行う際、認証ルールの選択は行わない。同様にＴＶ４４も、認証ルールの選択は行わない。

シンク１（５）としてＴＶ４４がソース３としてのＳＴＢ４２から送信されてくるＡＶデータの映像音声をモニタに表示しているものとする。

調査手段４３は、定期的に、シンク０（４）、シンク１（５）などＩＥＥＥ１３９４バス＃１（１）に接続されている機器毎のプラグの状態を調べている。

ここで、シンク１（５）が、ソース３から送信されてくるＡＶデータを受信して、デコード表示することを中止したとする。そうすると、そのＡＶデータに対応するｉＰＣＲのコネクションの設定が解除される。

調査手段４３は、シンク１（５）のｉＰＣＲの状態を調べた結果、シンク１（５）がソース３とのコネクションを切断したことがわかったとする。

そうすると、調査手段４３は、シンク１（５）のノードユニークＩＤを取得し、カウント調整・判定手段２６にシンク１（５）のノードユニークＩＤとシンク１（５）がソース３としてのＳＴＢ４２とのコネクションを切断したことを通知する。

これ以後の動作は第３の実施の形態と同様にして、従って、カウント調整・判定手段２６は、シンク１（５）のデバイスＩＤがすでにデバイス情報格納手段２７に格納されているので、デバイス情報格納手段２７からシンク１（５）のデバイスＩＤを削除し、また認証数カウント手段２４がカウントしている認証数を１だけカウントダウンするよう指示する。これを受けて認証数カウント手段２４は、カウントしている認証数を１だけカウントダウンする。

このように、第２の実施の形態とは異なり、ソース３から送信されているＡＶデータを受信して、デコード表示することを中止した機器を、ソース３であるＳＴＢ４２の調査手段４３が調査することによって、デクレメント認証をしなくても第２の実施の形態と同等の効果を得ることが出来る。

（第５の実施の形態）

次に、第５の実施の形態について説明する。

図１に本実施の形態の著作権保護システムを示す。

図５に本実施の形態のソース３をＳＴＢ４０として示す。本実施の形態のＳＴＢ４０は、第２の実施の形態で説明したものと同一である。

図３に、本実施の形態のＩＥＥＥ１３９４バス＃１（１）に接続されたシンク１（５）やＩＥＥＥ１３９４バス＃２（２）に接続されたシンク５（９）などをＴＶ３０として示す。本実施の形態のＴＶ３０は、第２の実施の形態で説明したものと同一である。

図１０に、シンク２（ブリッジ装置）（４）をブリッジ装置４６として示す。

ブリッジ装置４６は、ＩＥＥＥ１３９４バス＃１（１）から受信したアイソクロナスパケットとして送られてきたＡＶデータをいったん復号してから、ブリッジ装置４６が持つ鍵で暗号化してアイソクロナスパケットとしてＩＥＥＥ１３９４バス＃２（２）に送信し、このときＩＥＥＥ１３９４バス＃１（１）から受信したアイソクロナスパケットのヘッダに付加されている送信元のノードＩＤを自らのノードＩＤに書き換えて送信する装置である。

ブリッジ装置４６は、受信側Ｄ－Ｉ／Ｆ３１、復号手段３２、受信側認証手段３４、鍵カウント手段４７、認証要求手段４７、受信側認証ルール格納手段３６、受信側認証選択手段３５、送信側Ｄ－Ｉ／Ｆ２１、暗号化手段２２、送信側認証手段２３、認証数カウント手段４８、判定手段４１、デバイス情報格納手段２７、送信側認証ルール格納手段２９、送信側認証選択手段２８から構成される。

鍵カウント手段４７は、ＡＶデータをＩＥＥＥ１３９４バス＃１（１）に送信するソース３などの機器と認証を行い成功した数である鍵カウント数を数える手段である。

認証数カウント手段４８は、シンク５（９）などのＩＥＥＥ１３９４バス＃２（２）に接続されているシンク５（９）などの機器と認証を行い成功した数である認証数を数える手段である。

それ以外は、第２の実施の形態と同様であるので、説明を省略する。

なお、本実施の形態のブリッジ装置４６は本発明のブリッジ装置の例であり、本実施の形態の受信側認証ルール格納手段３６、受信側認証選択手段３５、受信側認証手段３４は本発明のブリッジ装置の受信側認証手段の例であり、本実施の形態の送信側認証ルール格納手段２９、送信側認証選択手段２８、送信側認証手段２３は本発明のブリッジ装置の送信側認証手段の例であり、本実施の形態の認証数カウント手段４８は本発明のブリッジ装置の認証数カウント手段の例であり、本実施の形態の認証数カウント手段４８がカウ

ントしている認証数は本発明のブリッジ装置の認証数カウント手段がカウントしている認証数の例であり本実施の形態の鍵カウント数は本発明の許可の上限数の例である。

次に、このような本実施の形態の動作を説明する。

図１１にブリッジ装置４６の動作を示すステートマシン図を示す。以下、このステートマシン図を参照して説明する。

ブリッジ装置４６は、ＩＥＥＥ１３９４バス＃１（１）においては、ソース３が送信したＡＶデータを受信するシンクとして機能し、ＩＥＥＥ１３９４バス＃２（２）においては、シンク５などにＡＶデータを送信するソースとして機能する。

ブリッジ装置４６の電源が入れられたり、ＩＥＥＥ１３９４バス＃１（１）とＩＥＥＥ１３９４バス＃２（２）にブリッジ装置４６が接続されるなどしてＩＥＥＥ１３９４バス＃２（２）のバスリセットが発生した場合、またＩＥＥＥ１３９４バス＃１（１）に機器が接続または取り外されるなどしてＩＥＥＥ１３９４バス＃１（１）にバスリセットが発生した場合、ブリッジ装置４６は未認証（Ｓ０）の状態にリセットされる。すなわち、ブリッジ装置の認証はリセットされる。未認証（Ｓ０）の状態では、ブリッジ装置４６の鍵カウント手段４７がカウントしている鍵カウント数は０に、ブリッジ装置４６の認証数カウント手段４８がカウントしている認証数は０にそれぞれ初期化される。

未認証（Ｓ０）の状態からソースとの認証（Ｓ１）への遷移では、認証の初期化が行われる。すなわち、ブリッジ装置３３の認証要求手段３３は、認証要求するためのコマンドである認証コマンドを作成し、受信側Ｄ－Ｉ／Ｆ３１に出力する。受信側Ｄ－Ｉ／Ｆ３１は、認証コマンドをＩＥＥＥ１３９４バス＃１（１）のソース３に送信する。

ソースとの認証（Ｓ１）の状態では、図５に示すソース３としてのＳＴＢ

４０は、第２の実施の形態と同様にして、ブリッジ装置４６からの認証コマンドを受信すると、認証コマンドを受理するか拒絶するかを判定する。そして、ＳＴＢ４０がブリッジ装置４６からの認証コマンドを拒絶した場合、またはブリッジ装置４６からの認証コマンドを受理したが認証に失敗した場合には、ソースとの認証（Ｓ１）の状態から未認証（Ｓ０）の状態に遷移する。

また、ＳＴＢ４０がブリッジ装置４６からの認証コマンドを受理し、ＳＴＢ４０の送信側認証手段２３と、ブリッジ装置４６の受信側認証手段３４が認証を行い成功した場合には、ソースとの認証（Ｓ１）の状態から認証済み（Ｓ２）の状態に遷移する。このとき、ブリッジ装置４６の鍵カウント手段４７は、カウントしている鍵カウント数を１だけカウントアップ、すなわち１にする。

また、ソース３としてのＳＴＢ４０の判定手段４１は、認証に成功したので、ＳＴＢ４０の認証数カウント手段２４がカウントしているカウント数を１だけカウントアップするよう指示し、これを受けて、ＳＴＢ４０の認証数カウント手段２４はカウントしている認証数を１だけカウントアップする。このようなＳＴＢ４０の動作については第２の実施の形態で詳細に説明した。

認証済み（Ｓ２）の状態では、ブリッジ装置４６はソース３などと認証が成功した状態にある。

認証済み（Ｓ２）の状態で、ＩＥＥＥ１３９４＃２（２）に接続されたシンク５（９）などの機器から認証要求されると、ブリッジ装置４６の判定手段４１は、次のように判断する。すなわち、現在ブリッジ装置の認証数カウント手段４８がカウントしている認証数が０であり、鍵カウント手段４７がカウントしている鍵カウント数が１でありので、認証数の方が鍵カウント数より値が小さくなっている。この場合、シンク５（９）からの認証コマンドに応じて、ブリッジ装置４６の送信側認証手段２３がシンク５（９）と認証を行うべきと判定する。ブリッジ装置４６の送信側認証手段２３は、この判

定に従って、シンク５（９）と認証を行う。すなわち、認証済み（Ｓ２）の状態からシンクまたは別ブリッジ（受信側）との認証（Ｓ３）の状態に遷移する。ブリッジ装置４６の送信側認証手段２３とシンク５（９）との認証が成功すると、ブリッジ装置４６の認証数カウント手段４８はカウントしている認証数を１だけカウントアップし、デバイス情報格納手段２７は、シンク５（９）のデバイスＩＤを格納する。従って、鍵カウント手段４７がカウントている鍵カウント数は１であり、認証数カウント手段４８がカウントしている認証数は１になった。そして、認証済み（Ｓ２）の状態に遷移する。

ここで、さらに、シンク６（１０）がブリッジ装置４６に認証コマンドを送信したとする。この場合、ブリッジ装置４６の送信側認証手段２３がシンク６（１０）からの認証コマンドを受け取ると、ブリッジ装置４６の判定手段４１は送信側認証手段２３からの依頼に基づいて、次のように判定する。すなわち、現在、鍵カウント手段４７がカウントしている鍵カウント数が１であり、ブリッジ装置４６の認証数カウント手段４８がカウントしている認証数も１であり、鍵カウント数と認証数が等しくなっている。鍵カウント数と認証数が等しい場合、判定手段４１は、シンク６（１０）からの認証要求をリトライ終了させ、まず、ソース３と認証を行うべきと判定する。送信側認証手段２３はこの判定に従って、シンク６（１０）からの認証要求をいったん拒絶して終了させる。そして、ブリッジ装置４６の認証要求手段３３はソース３に認証コマンドを送信する。すなわち、認証済み（Ｓ２）の状態からソースとの認証（Ｓ４）の状態に遷移する。

第２の実施の形態では、説明しなかったが、ブリッジ装置４６はＩＥＥＥ１３９４バス＃１（１）のシンク２（６）として、他のシンク５（９）などとは異なり重複して認証要求をソース３に行う。そして、ソース３としてのＳＴＢ４０は、ブリッジ装置４６と認証を行い成功する度に、認証上限数格納手段２５の上限数を越えない範囲で、ＳＴＢ４０の認証数カウント手段２

４はカウントしている認証数をカウントアップする。ＳＴＢ４０の判定手段４１が認証要求を受理するか拒絶するかの判定はブリッジ装置４６とシンク１（５）などの場合で全く同様に行う。

ソース３とブリッジ装置４６の送信側認証手段３４とが第２の実施の形態と同様にして認証を行い成功すると、鍵カウント手段４７は、カウントしている鍵カウントを１だけカウントアップする。すなわち、ソースとの認証（Ｓ４）の状態から認証済み（Ｓ２）の状態に遷移する。この時点で、鍵カウント数は２になっており、認証数は１になっている。

認証済み（Ｓ２）の状態で、シンク６（１０）から再び認証コマンドを受信すると、ブリッジ装置４６の判定手段４１は、鍵カウント数が認証数より大きいので、シンク６（１０）と認証すべきと判定する。すなわち、認証済み（Ｓ２）の状態からシンクまたは別ブリッジ（受信側）との認証（Ｓ３）の状態に遷移する。そして、シンクまたは別ブリッジ（受信側）との認証（Ｓ３）の状態で、ブリッジ装置４６の送信側認証手段２３がシンク６（１０）と認証を行い成功すると、ブリッジ装置４６の認証数カウント手段４８は、カウントしている認証数を１だけカウントアップし、デバイス情報格納手段２７は、シンク６（１０）のデバイスＩＤを格納する。そして、シンクまたは別ブリッジ（受信側）との認証（Ｓ３）の状態から認証済み（Ｓ２）の状態に遷移する。この状態で鍵カウント数は２であり、認証数は２になっている。

このようにブリッジ装置４６がＩＥＥＥ１３９４バス＃２に接続されている機器から認証要求された際、ブリッジ装置４６は、鍵カウント数が認証数より大きい場合、認証済み（Ｓ２）の状態からシンクまたは別ブリッジ（受信側）との認証（Ｓ３）の状態に遷移し、鍵カウント数と認証数が等しい場合には、その機器からの認証要求をリトライ終了させ、ソース３にと認証を

行う。すなわち、認証済み（Ｓ２）の状態からソースとの認証（Ｓ４）の状態に遷移する。すなわち、ブリッジ装置４６は、ＩＥＥＥ１３９４バス＃２（２）に接続された機器から認証要求された場合、鍵カウント数と認証数の値を比較し、鍵カウント数の方が認証数より大きい場合には、ＩＥＥＥ１３９４バス＃２（２）に接続された機器と認証を行い、鍵カウント数と認証数が等しい場合には、認証要求した機器と認証を行う前に、ソース３と認証を行う。

また、ＩＥＥＥ１３９４バス＃１に接続されているソース３は、第２の実施の形態で説明したように、同時に最大３台までの機器にのみＡＶデータをデコード表示出来るように制限する機器である。このように、ブリッジ装置４６は、ＩＥＥＥ１３９４バス＃２に接続されたシンクから認証要求された場合、その機器と認証を行う前にＩＥＥＥ１３９４バス＃１に接続されたソースと認証を行い、その認証が成功してから、ＩＥＥＥ１３９４バス＃２に接続されたシンクと認証を行うので、ブリッジ装置４６が存在していてもソース３から送信された著作権保護が必要なＡＶデータの台数の制限を守ることが出来る。

さて、シンク５（９）がソース３から送信された著作権保護が必要なＡＶデータを受信してデコードし、モニタに表示することを中止するシンク５（９）は、第１の実施の形態で説明したのと同様にして、ブリッジ装置４６にデクレメント認証用コマンドを送信することによってデクレメント認証を要求する。すなわち、認証済み（Ｓ２）の状態からシンクまたは別ブリッジ（受信側）とのデクレメント認証（Ｓ５）の状態に遷移する。この時点で、鍵カウント手段４７の鍵カウント数は２であり、ブリッジ装置４６の認証数カウント手段４８がカウントしている認証数も２である。

シンクまたは別ブリッジ（受信側）とのデクレメント認証（Ｓ５）の状態では、ブリッジ装置４６は、シンク５（９）とデクレメン認証を行う。そし

て、デクレメント認証に成功した場合、ブリッジ装置４６の認証数カウント手段４８がカウントしている認証数を１だけカウントダウンし、デバイス情報格納手段２７は、格納しているシンク５（９）のデバイスＩＤを削除する。そして、シンクまたは別ブリッジ（受信側）とのデクレメント認証（Ｓ５）の状態からソースとのデクレメント認証（Ｓ６）の状態に遷移する。一方、デクレメント認証に失敗した場合にはシンクまたは別ブリッジ（受信側）とのデクレメント認証（Ｓ５）から認証済み（Ｓ２）の状態に遷移する。

ソースとのデクレメント認証（Ｓ６）の状態では、ブリッジ装置４６はソース３とデクレメント認証を行い、成功すると、鍵カウント数を１だけカウントダウンし、ソースとのデクレメント認証（Ｓ６）の状態から認証済み（Ｓ２）の状態に遷移する。また、デクレメント認証が失敗すると、鍵カウント数をカウントダウンせずにソースとのデクレメント認証（Ｓ６）の状態から認証済み（Ｓ２）の状態に遷移する。この時点で、鍵カウント数は１になり、ブリッジ装置４６の認証数も１になっている。

引き続き、認証済み（Ｓ２）の状態で、ＩＥＥＥ１３９４バス＃２に接続されている他の機器から認証要求やデクレメント認証要求された場合、上記の動作を繰り返す。

このように、ＩＥＥＥ１３９４バス＃２（２）に接続された機器がＡＶデータを受信してデコード表示することを中止する場合、第２の実施の形態と同様にしてそのことをブリッジ装置４６に申告し、ブリッジ装置４６がデクレメント認証を行うことによって、ＩＥＥＥ１３９４バス＃１（１）とＩＥＥＥ１３９４バス＃２（２）がブリッジ装置と接続されていても、第２の実施の形態と同様にＩＥＥＥ１３９４バス＃１（１）とＩＥＥＥ１３９４バス＃２（２）に接続されている機器が、新たにＡＶデータを使用することが出来るようになる。

ところで、ＩＥＥＥ１３９４では、ソース３は、アイソクロナスリソース

マネージャから帯域とチャンネルを割り当てられたら即アイソクロナスパケットを送らなければならない。ソース３は、送るべきＡＶデータがない場合は空のアイソクロナスパケットをＩＥＥＥ１３９４バス＃１に送る。そして、ソース３が空のアイソクロナスパケットさえもＩＥＥＥ１３９４バス＃１に送らなかった場合、ＤＴＣＰ方式では、ソース３の認証がリセットされる。

従って、ブリッジ装置４６（Ｓ２）が、認証済み（Ｓ２）の状態にあり、ソース３からのアイソクロナスパケットの送信が途切れた場合、認証済み（Ｓ２）の状態から遷移し、鍵カウンタを０に初期化し、またブリッジ装置４６の認証数カウント手段４８がカウントしている認証数を０に初期化し、認証済み（Ｓ２）の状態に戻る。すなわち、ソース３の認証がリセットされると、ブリッジ装置４６も認証をリセットする。

また、ソース３からのアイソクロナスパケットの送信は継続しているが、ブリッジ装置４６からのアイソクロナスパケットの送信が途切れた場合、認証済み（Ｓ２）の状態から遷移し、ブリッジ装置４６の認証数カウント手段２３がカウントしている認証数を０に初期化して、再び認証済み（Ｓ２）の状態に戻る。すなわち、ブリッジ装置４６は認証をリセットする。

また、認証済み（Ｓ２）の状態にあり、ＩＥＥＥ１３９４バス＃２（２）に接続されているシンク５（９）などの機器がＩＥＥＥ１３９４バス＃２（２）から消失したことをブリッジ装置４６が発見した場合、認証済み（Ｓ２）の状態からソースとのデクレメント認証（Ｓ６）の状態に遷移する。

そして、ソースとのデクレメント認証（Ｓ６）の状態で、ブリッジ装置４６は、ソース３とデクレメント認証を行う。成功した場合に鍵カウント数を１だけカウントダウンし、認証済み（Ｓ２）の状態に遷移する。失敗した場合は、鍵カウント数をカウントダウンせずに認証済み（Ｓ２）の状態に遷移する。

このように、ブリッジ装置４６がＩＥＥＥ１３９４バス＃１（１）とＩＥ

ＥＥ１３９４バス＃２を接続している場合であっても、第２の実施の形態で説明したのと同等の効果を得ることが出来る。

なお、本実施の形態では、ブリッジ装置４６は、ＩＥＥＥ１３９４バス＃２（２）に接続されている機器から認証要求された場合、鍵カウント手段４７がカウントしている鍵カウント数とブリッジ装置４６の認証数カウント手段４８がカウントしている認証数との大小関係に基づいて、その機器と認証するか、その機器と認証する前にソース３と認証を行うかを判定したが、これに限らない。鍵カウント手段４７を設けず、ＩＥＥＥ１３９４バス＃２（２）に接続されているシンクから認証要求された場合、その認証を行う前にソース３と認証し、ソース３との認証が成功した場合のみ、そのシンクと認証を行っても構わない。このようにしても本実施の形態と同等の効果を得ることが出来る。

（第６の実施の形態）

次に、第６の実施の形態について説明する。

本実施の形態の著作権保護システムを第５の実施の形態と同様に図１に示す。

図５に本実施の形態のソース３を、ＳＴＢ４０として示す。ＳＴＢ４０は第２の実施の形態で説明したものと同一である。

また、図３に、本実施の形態のＩＥＥＥ１３９４バス＃１（１）に接続されたシンク１（５）やＩＥＥＥ１３９４バス＃２（２）に接続されたシンク５（９）などをＴＶ３０として示す。ＴＶ３０は第２の実施の形態で説明したものと同一である。

また、図１０に、シンク２（ブリッジ装置）（４）として、ブリッジ装置４６を示す。

本実施の形態のブリッジ装置４６は第５の実施の形態と同様の構成を持つ。

次に、このような本実施の形態の動作を第５の実施の形態との相違点を中

心に説明する。

第５の実施の形態では、ブリッジ装置４６は図１１のステートマシン図において、未認証（Ｓ０）の状態からソースとの認証（Ｓ１）の状態、認証済み（Ｓ２）へ遷移する際、ソース３と一回だけ認証を行い、成功した場合鍵カウント手段４７がカウントしている鍵カウント数は１に設定された。

これに対して本実施の形態では、未認証（Ｓ０）の状態からソースとの認証（Ｓ１）の状態、認証済み（Ｓ２）へ遷移する際、ブリッジ装置４６の認証要求手段３３は、ソース３と認証したい回数を付加した認証コマンドをソース３に送信する。

そして、ブリッジ装置４６の受信側認証手段３４は、認証要求する際に指定した回数だけソース３と認証を行う。一方、ソース３はブリッジ装置４６の受信側認証手段３４と認証を行う際、第２の実施の形態と同様に認証上限数格納手段２５に格納されている上限数と、ＳＴＢ４０の認証数カウント手段２４がカウントしている認証数に基づき、ブリッジ装置４６からの認証を拒絶するか認証を行うかを判定して認証を行う。

ブリッジ装置４６がこのように指定した回数だけまとめて認証を行い成功した回数分だけ、鍵カウント手段４７は、鍵カウント数をカウントアップする。

従って、上記の認証が成功した場合、認証済み（Ｓ２）の状態に遷移した時点で、認証要求手段３３が認証コマンドに付加したソース３と認証したい回数が１より大きい場合、鍵カウント数は１より大きい値になっており、またブリッジ装置４８の認証数カウント手段４８の認証数は、０になっている。

これ以外は、第５の実施の形態と同様である。すなわち、本実施の形態のブリッジ装置４６は認証したい回数をソース３に通知し、その回数だけ予め認証するので、ＩＥＥＥ１３９４＃２（２）に接続されたシンク５などの機器から認証要求されても、その認証要求を一旦拒絶し、ソース３と認証し成

功してから再度、その認証要求した機器と認証を行うといった２段階の処理を行う必要がない。予めソース３と認証した回数分までは、ＩＥＥＥ１３９４バス＃２（２）に接続されたシンク５などの機器からの認証要求を即座に受理して、その機器と認証を行うことが出来る。従って、第５の実施の形態と同等の効果に加え、さらに、ブリッジ装置４６の認証要求に対する応答時間が短くなるという効果も得ることが出来る。

（第７の実施の形態）

次に、第７の実施の形態について説明する。

本実施の形態の著作権保護システムを第５の実施の形態と同様に図１に示す。

図５に本実施の形態のソース３を、ＳＴＢ４０として示す。ＳＴＢ４０は第２の実施の形態で説明したものと同一である。

また、図３に、本実施の形態のＩＥＥＥ１３９４バス＃１（１）に接続されたシンク１（５）やＩＥＥＥ１３９４バス＃２（２）に接続されたシンク５（９）などをＴＶ３０として示す。ＴＶ3.0は第２の実施の形態で説明したものと同一である。

また、図１０に、シンク２（ブリッジ装置）（６）として、ブリッジ装置４６を示す。

本実施の形態のブリッジ装置４６は第５の実施の形態と同様の構成を持つ。

次に、このような本実施の形態の動作を第５の実施の形態との相違点を中心に説明する。

第５の実施の形態では、ＩＥＥＥ１３９４バス＃２に接続されている機器からデクレメント認証を要求された場合、認証済み（Ｓ２）の状態からシンクまたは別ブリッジ（受信側）とのデクレメント認証（Ｓ５）の状態に遷移し、さらにソースとのデクレメント認証（Ｓ６）の状態に遷移し、再び認証済み（Ｓ２）の状態に遷移した。

すなわち、ブリッジ装置４６は、ＩＥＥＥ１３９４バス＃２（２）に接続されている機器とデクレメント認証を行って成功した場合、ブリッジ装置４６の認証数カウント手段４８がカウントしている認証数を１だけカウントダウンし、引き続いて、ソース３とデクレメント認証を行って成功した場合、鍵カウント手段４７がカウントしている鍵カウント数を１だけカウントダウンした。

これに対して本実施の形態では、ＩＥＥＥ１３９４バス＃２からデクレメント認証を要求された場合、認証済み（Ｓ２）の状態からシンクまたは別ブリッジ（受信側）とのデクレメント認証（Ｓ５）に遷移する。すなわち、ブリッジ装置４６は、ＩＥＥＥ１３９４バス＃２に接続されている機器とデクレメント認証を行い、その結果成功した場合、ブリッジ装置４６の認証数カウント手段４８がカウントしている認証数を１だけカウントダウンする。

次に、ソースとのデクレメント認証（Ｓ６）には遷移せず、認証済み（Ｓ２）の状態に遷移する。すなわち、引き続き、ソース３とはデクレメント認証しない。従って、鍵カウント手段４７がカウントしている鍵カウント数は変化しない。

上記のデクレメント認証が行われてから、新たにＩＥＥＥ１３９４バス＃２に接続されている機器から認証要求されない時間が所定の時間、例えば５分間経過すると、ブリッジ装置４６はソースとのデクレメント認証を行う。

まだ、ソースとのデクレメント認証をブリッジ装置４６が行っていない状態で、ＩＥＥＥ１３９４バス＃２（２）に接続されているシンク７（１１）などの機器から認証要求された場合、認証数が鍵カウント数より値が小さいので、ブリッジ装置４６は、その認証要求した機器と認証を行う前に、ソース３と認証を行う必要がないので、ブリッジ装置４６は、第５の実施の形態に比較してＩＥＥＥ１３９４バス＃２（２）からの認証要求に対して素早く応答することが出来る。

従って、第５の実施の形態と同等の効果に加え、さらに、ブリッジ装置４６の認証要求に対する応答時間が短くなるという効果も得ることが出来る。

なお、本発明は、上述した本発明の著作権保護システムの全部または一部の手段（または、装置、素子、回路、部等）の機能をコンピュータにより実行させるためのプログラムであって、コンピュータと協働して動作するプログラムである。

本発明は、上述した本発明の著作権保護システムの全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラムを担持した媒体であり、コンピュータにより読み取り可能且つ、読み取られた前記プログラムが前記コンピュータと協動して前記機能を実行する媒体である。

なお、本発明の一部の手段（または、装置、素子、回路、部等）、本発明の一部のステップ（または、工程、動作、作用等）とは、それらの複数の手段またはステップの内の、幾つかの手段またはステップを意味し、あるいは、一つの手段またはステップの内の、一部の機能または一部の動作を意味するものである。

また、本発明の一部の装置（または、素子、回路、部等）とは、それらの複数の装置の内の、幾つかの装置を意味し、あるいは、一つの装置の内の、一部の手段（または、素子、回路、部等）を意味し、あるいは、一つの手段の内の、一部の機能を意味するものである。

また、本発明のプログラムを記録した、コンピュータに読みとり可能な記録媒体も本発明に含まれる。

また、本発明のプログラムの一利用形態は、コンピュータにより読み取り可能な記録媒体に記録され、コンピュータと協働して動作する態様であっても良い。

また、本発明のプログラムの一利用形態は、伝送媒体中を伝送し、コ

ンピュータにより読みとられ、コンピュータと協働して動作する態様であっても良い。

また、本発明のデータ構造としては、データベース、データフォーマット、データテーブル、データリスト、データの種類などを含む。

また、記録媒体としては、ＲＯＭ等が含まれ、伝送媒体としては、インターネット等の伝送媒体、光・電波・音波等が含まれる。

また、上述した本発明のコンピュータは、ＣＰＵ等の純然たるハードウェアに限らず、ファームウェアや、ＯＳ、更に周辺機器を含むものであっても良い。

なお、以上説明した様に、本発明の構成は、ソフトウェア的に実現しても良いし、ハードウェア的に実現しても良い。

産業上の利用可能性

以上説明したところから明らかなように、本発明は、ネットワークにブリッジ装置が接続されていても、著作権保護が必要な信号を受け取ることが出来る受信機器の数を制限したいという著作権者の要望を守ることが出来る著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムを提供することが出来る。

また、本発明は、著作権保護が必要な信号をうけとることが出来る受信機器の数を受信機器の台数を指定して制限するという著作権者の要望を守ることが出来る著作権保護システム、送信装置、受信装置、ブリッジ装置、著作権保護方法、媒体及びプログラムを提供することが出来る。

請　　求　　の　　範　　囲

１．　ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも１台以上の受信装置と、

前記受信装置に、前記ネットワークを利用して前記著作権保護が必要なデータを送信する送信装置とを備えた著作権保護システムであって、

前記送信装置は、前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記受信装置は、前記送信側認証手段と認証を行う受信側認証手段を有し、

前記認証数に制限を設けたことを特徴とする著作権保護システム。

２．　前記認証数カウント手段は、前記送信側認証手段が認証を行い成功すると、前記認証数を加算することを特徴とする請求項１記載の著作権保護システム。

３．　前記受信装置は、前記送信装置と認証を行い成功した場合、所定の原因によって前記認証がリセットされない限り、再度認証要求しないことを特徴とする請求項２記載の著作権保護システム。

４．　前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置は、再度認証要求することが出来ることを特徴とする請求項３記載の著作権保護システム。

５．　前記送信装置は、前記受信装置と認証を行い成功した場合、所定の

原因によって前記認証がリセットされない限り、再度前記受信装置から認証要求があってもその認証要求を受け付けないことを特徴とする請求項２記載の著作権保護システム。

６．　前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置は、前記ブリッジ装置から認証要求が行われた場合、その認証要求を受け付けることを特徴とする請求項５記載の著作権保護システム。

７．　前記送信装置は、前記受信装置と認証を行い成功した場合、再度前記受信装置と認証を行うが、所定の原因によって前記認証がリセットされない限り、たとえその認証に成功しても前記認証数カウント手段は、前記認証数を加算しないことを特徴とする請求項２記載の著作権保護システム。

８．　前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記認証数カウント手段は、再度前記ブリッジ装置と認証を行い成功した場合、前記認証数を加算することを特徴とする請求項７記載の著作権保護システム。

９．　前記送信側認証手段は、前記受信装置と認証を行い成功した場合、前記受信装置を特定する情報を登録する登録手段と、

前記受信装置から認証要求が行われると、その認証要求がすでに認証を行い成功した前記受信装置からの認証要求かどうかを登録した前記受信装置を特定する情報を利用して行う重複判定手段とを有することを特徴とする請求項３～８のいずれかに記載の著作権保護システム。

１０．　前記認証のリセットは、鍵の更新が行われた時に起こることを特徴とする請求項３～８のいずれかに記載の著作権保護システム。

１１．　前記認証のリセットは、交換鍵の更新が行われた時に起こることを特徴とする請求項３～８のいずれかに記載の著作権保護システム。

１２．　前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置が前記鍵の更新を行った場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする請求項１０記載の著作権保護システム。

１３．　前記認証のリセットは、バスリセットされた際に起こることを特徴とする請求項３～８のいずれかに記載の著作権保護システム。

１４．　前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記送信装置が接続されている前記ネットワークで、前記バスリセットされた場合、前記他のネットワークでも前記認証のリセットが行われることを特徴とする請求項１３記載の著作権保護システム。

１５．　前記認証数に制限を設けるとは、前記認証数が所定の値以上になった場合、前記送信側認証手段は、前記受信装置からの認証要求を受け付けないことであることを特徴とする請求項１記載の著作権保護システム。

１６．　前記送信側認証手段と認証を行い成功した前記受信装置が、前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止した場合、前記認証数カウント手段は、前記認証数を減算することを特徴とする請

求項１記載の記載の著作権保護システム。

１７．　前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられており、

そのブリッジ装置は、前記送信装置が接続された前記ネットワークでは、前記受信装置として扱われ、

前記ブリッジ装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止するとは、前記他のネットワークに接続されているすべての前記受信装置が前記送信装置から送られてくる前記著作権の保護が必要なデータの使用を中止したことであることを特徴とする請求項１６記載の著作権保護システム。

１８．　前記送信装置は、前記送信側認証手段と認証を行い成功した前記受信装置を特定する情報を登録する登録手段を有し、

前記認証数カウント手段が前記認証数を減算した場合、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録を解除することを特徴とする請求項１６記載の著作権保護システム。

１９．　前記送信装置は、前記受信装置が、前記著作権保護が必要なデータの使用を中止したかどうかを調査する調査手段を有することを特徴とする請求項１６記載の著作権保護システム。

２０．　前記著作権保護が必要なデータの使用を中止するとは、前記受信装置が前記ネットワークから切り離されることであり、

前記調査手段は、前記受信装置が前記ネットワークから切り離されたかどうかを定期的に調査することを特徴とする請求項１９記載の著作権保護システム。

２１．　前記調査するとは、前記ネットワークに接続されている前記受信装置の数である接続数を定期的に調査し、前記接続数が減少した場合、どの前記受信装置が前記ネットワークから切り離されたかをチェックすることであ

ることを特徴とする請求項２０記載の著作権保護システム。

２２．　前記調査手段は、前記受信装置の動作状態及び／または接続プラグのアクティブ状態を調べることによって、前記受信装置が前記著作権保護が必要なデータの使用を中止したかをチェックし、

前記認証数カウント手段は、前記調査手段の調査の結果、前記受信装置が前記著作権保護が必要なデータを使用していないようであれば、前記認証数を減算することを特徴とする請求項１９記載の著作権保護システム。

２３．　前記調査手段は、前記受信装置を特定する情報と、その受信装置の署名とを対応付ける対応表を有し、

前記調査手段は、前記対応表を利用して、前記ネットワークから切り離された前記受信装置が認証済みであったかどうかを判定し、

前記認証数カウント手段は、前記判定結果が、前記ネットワークからきりはなされた前記受信装置が認証済みであったことを示す場合、前記認証数を減算することを特徴とする請求項２０または２１に記載の著作権保護システム。

２４．　前記受信側認証手段は、前記受信装置が前記送信装置から送られてくる前記著作権保護が必要なデータの使用を中止する場合、前記送信装置に前記認証数を減算するためのデクレメント認証要求を行い、

前記送信側認証手段は、前記受信側認証手段と、前記デクレメント認証を行い、

前記認証数カウント手段は、前記デクレメント認証が成功すると、前記認証数を減算することを特報とする請求項１６記載の著作権保護システム。

２５．　前記デクレメント認証を行うためのコマンドであるデクレメント認証用コマンドが、前記著作権保護が必要なデータを使用する際の認証を行うためのコマンドである認証コマンドとは別に作成されていることを特徴とする請求項２４記載の著作権保護システム。

２６．　前記著作権保護が必要なデータは暗号化されており、

前記デクレメント認証が成功すると、前記受信装置は、前記著作権保護が必要なデータを解読するための鍵を放棄することを特徴とする請求項２４または２５に記載の著作権保護システム。

２７．　前記デクレメント認証は、前記著作権保護が必要なデータを使用するための認証とは、署名、認証方法、演算式の少なくとも１つ以上が異なっていることを特徴とする請求項２４または２５に記載の著作権保護システム。

２８．　所定の原因によって認証がリセットされた場合、前記認証数カウント手段は、前記認証数を初期化し、前記登録手段は、前記送信側認証手段と認証を行い成功した受信装置を特定する情報の登録をすべて解除することを特徴とする請求項１８記載の著作権保護システム。

２９．　前記ネットワークを他のネットワークに接続するためのブリッジ装置が設けられていることを特徴とする請求項２記載の著作権保護システム。

３０．　前記ブリッジ装置は、前記他のネットワークでは、前記送信装置として扱われ、

前記他のネットワークに接続された前記受信装置から認証要求が行われた場合、

その受信装置と認証を行う前に、前記ネットワークに接続された前記送信装置と認証を行い、その送信装置との認証が成功した場合、前記受信装置と認証を行うことを特徴とする請求項２９記載の著作権保護システム。

３１．　前記ブリッジ装置の前記認証数カウント手段が減算された場合、前記ブリッジ装置は、前記ネットワークに接続された前記送信装置と、前記ネットワークに接続された前記送信装置の前記認証数カウント手段がカウントしている前記認証数を減算させるためのデクレメント認証を行うことを特徴とする請求項２９記載の著作権保護システム。

３２．　前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置

の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントすることを特徴とする請求項２９記載の著作権保護システム。

３３．　前記ネットワークに新たに前記送信装置が接続された場合、前記ブリッジ装置は、前記ブリッジ装置の前記認証数カウント手段がカウントしていた前記認証数の回数だけ新たに接続された前記送信装置と認証を行うことを特徴とする請求項３２記載の著作権保護システム。

３４．　前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を有し、

前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である前記認証数をカウントし、

前記ブリッジ装置は、前記ネットワークに接続された前記送信装置と認証して成功した数を前記鍵カウンタがカウントしている前記許可の限度数とし、

前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数を減算するためのデクレメント認証要求があった場合、前記ブリッジ装置は前記ネットワークに接続されている前記送信装置とデクレメント認証を行わず、その受信装置とデクレメント認証を行い、

前記デクレメント認証が成功すると、前記ブリッジ装置の前記認証数カウント手段は、前記認証数を減算し、

前記他のネットワークに接続されている前記受信装置から新たに認証要求があった際、

前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウン

トしている前記認証数より小さい場合には、その受信装置と認証を行い、

前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より小さくない場合には、その受信装置と認証を行う前に前記ネットワークに接続されている前記送信装置と認証を行い、その認証が成功した場合、その受信装置と認証を行うことを特徴とする請求項３０記載の著作権保護システム。

３５．　前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から送られてくるデータを再暗号化して、前記他のネットワークに接続されている前記受信装置に送信し、

前記ブリッジ装置の前記認証数カウント手段は、前記ブリッジ装置の前記送信側認証手段が前記他のネットワークに接続された前記受信装置と認証を行い成功した数である認証数をカウントし、

前記ブリッジ装置は、前記ネットワークに接続されている前記送信装置から割り当てられた許可の限度数をカウントする鍵カウント手段を有することを特徴とする請求項２９記載の著作権保護システム。

３６．　前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数と前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きい場合、その認証要求を許可することを特徴とする請求項３５記載の著作権保護システム。

３７．　前記鍵カウント手段がカウントしている許可の限度数の上限は予め前記ネットワークに接続されている前記送信装置から与えられていることを特徴とする請求項３６記載の著作権保護システム。

３８．　前記鍵カウント手段がカウントしている許可の限度数の上限は、前記ブリッジ装置が前記ネットワークに接続されている前記送信装置と認証を

行うことによって、加算されることを特徴とする請求項３６記載の著作権保護システム。

３９．　前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、その認証要求を拒絶することを特徴とする請求項３５記載の著作権保護システム。

４０．　前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に前記許可の限度数を加算するよう依頼することを特徴とする請求項３５記載の著作権保護システム。

４１．　前記ブリッジ装置は、前記他のネットワークに接続されている前記受信装置から認証要求があった場合、前記鍵カウント手段がカウントしている前記許可の限度数が前記ブリッジ装置の前記認証数カウント手段がカウントしている前記認証数より大きくない場合、前記ネットワークに接続されている前記送信装置に認証要求を行い、前記認証が成功した場合、前記鍵カウント手段は、前記許可の限度数を加算することを特徴とする請求項３５記載の著作権保護システム。

４２．　前記ブリッジ装置は、前記他のネットワークに接続された前記受信装置から認証要求される毎に、前記ネットワークに接続された前記送信装置に前記他のネットワークに接続された前記受信装置のうち認証要求を行っているものの台数を通知することを特徴とする請求項２９記載の著作権保護システム。

４３．　前記ブリッジ装置が前記ネットワークに接続された前記送信装置に

対して認証要求を行うための認証コマンドには、前記台数を通知するためのフィールドが設けられており、前記ブリッジ装置は、前記フィールドを利用して前記台数の通知を行うことを特徴とする請求項４２記載の著作権保護システム。

４４．　前記ブリッジ装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドは、前記ブリッジ装置の機能を有しない前記ネットワークに接続された前記受信装置が前記ネットワークに接続された前記送信装置に対して認証要求を行うための認証コマンドとは区別されていることを特徴とする請求項２９記載の著作権保護システム。

４５．　前記区別は、前記認証コマンドに添付する署名によって行われることを特徴とする請求項４４記載の著作権保護システム。

４６．　送信装置と認証する受信側認証手段を有し、ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも１台以上の受信装置に対して、前記ネットワークを利用して前記著作権保護が必要なデータを送信する送信装置であって、

前記受信側認証手段と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記認証数に制限を設けたことを特徴とする送信装置。

４７．　ネットワークに接続され、著作権保護が必要なデータを受信して使用する受信装置であって、

前記受信装置と認証を行う送信側認証手段と、前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有する送信装置の前記送信側認証手段と認証する受信側認証手段を備え、

前記認証数に制限を設けたことを特徴とする受信装置。

４８．　前記一方のネットワークに接続された送信装置から送信された著作

権保護が必要なデータを前記他のネットワークに接続された受信装置に送信するブリッジ装置であって、

前記受信装置と認証を行うブリッジ装置用送信側認証手段と、

前記送信側認証手段が認証した数であるブリッジ装置用認証数を数えるブリッジ装置用認証数カウント手段と、

前記送信装置と認証を行うブリッジ装置用受信側認証手段とを備え、

前記送信装置は、前記ブリッジ装置または前記ネットワークに接続された前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段とを有し、

前記受信装置は、前記ブリッジ装置または前記他のネットワークに接続された前記送信装置と認証する受信側認証手段を有し、

前記送信側認証手段が数える前記認証数に制限を設けたことを特徴とするブリッジ装置。

４９．　ネットワークに接続され、著作権保護が必要なデータを受信して使用する少なくとも一台以上の受信装置に、前記ネットワークを利用して送信装置から前記著作権保護が必要なデータを送信する著作権保護方法であって、

前記送信装置は、前記受信装置と認証した数である認証数を数え、

前記認証数に制限を設けたことを特徴とする著作権保護方法。

５０．　請求項１記載の著作権保護システムの、前記受信装置における、前記送信側認証手段と認証を行う受信側認証手段と、

前記送信装置における、前記受信装置と認証を行う送信側認証手段と、

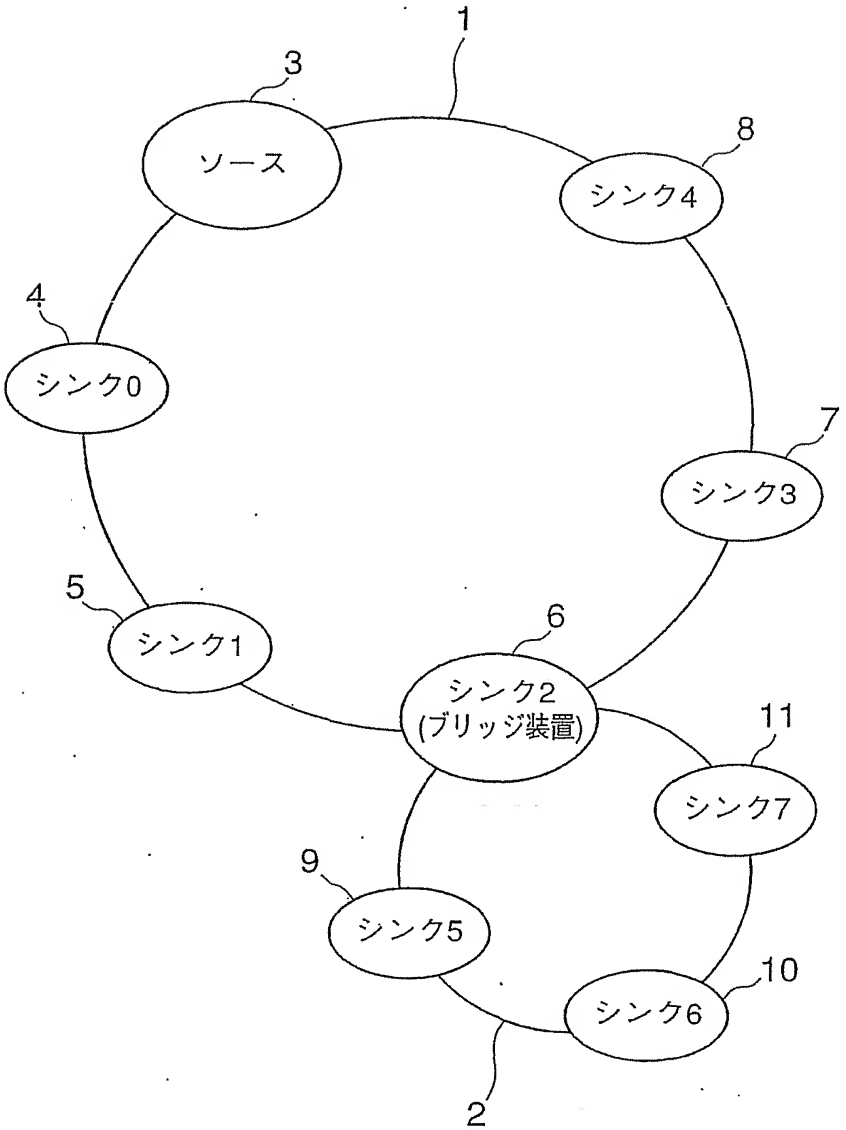
前記送信側認証手段が認証した数である認証数を数える認証数カウント手段との全部または一部としてコンピュータを機能させるためのプログラムを担持した媒体であって、コンピュータにより処理可能である媒体。

５１．　請求項１記載の著作権保護システムの、前記受信装置における、前記送信側認証手段と認証を行う受信側認証手段と、

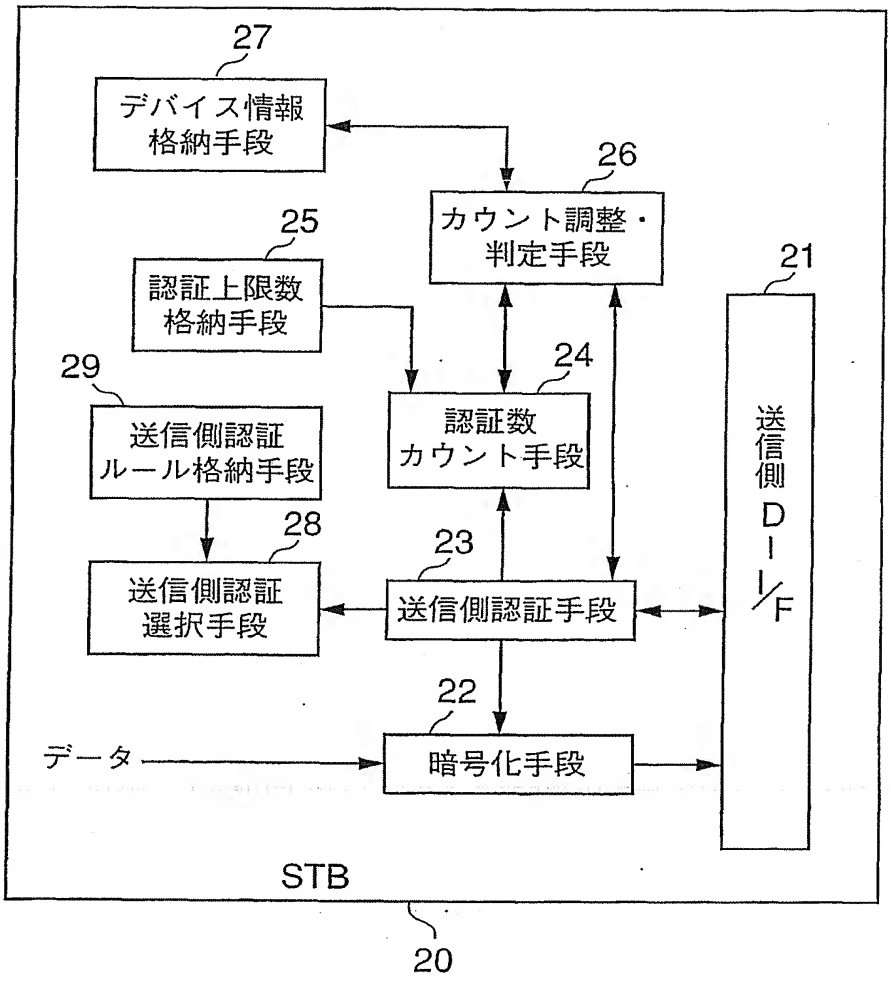
前記送信装置における、前記受信装置と認証を行う送信側認証手段と、

前記送信側認証手段が認証した数である認証数を数える認証数カウント手段との全部または一部としてコンピュータを機能させるためのプログラム。

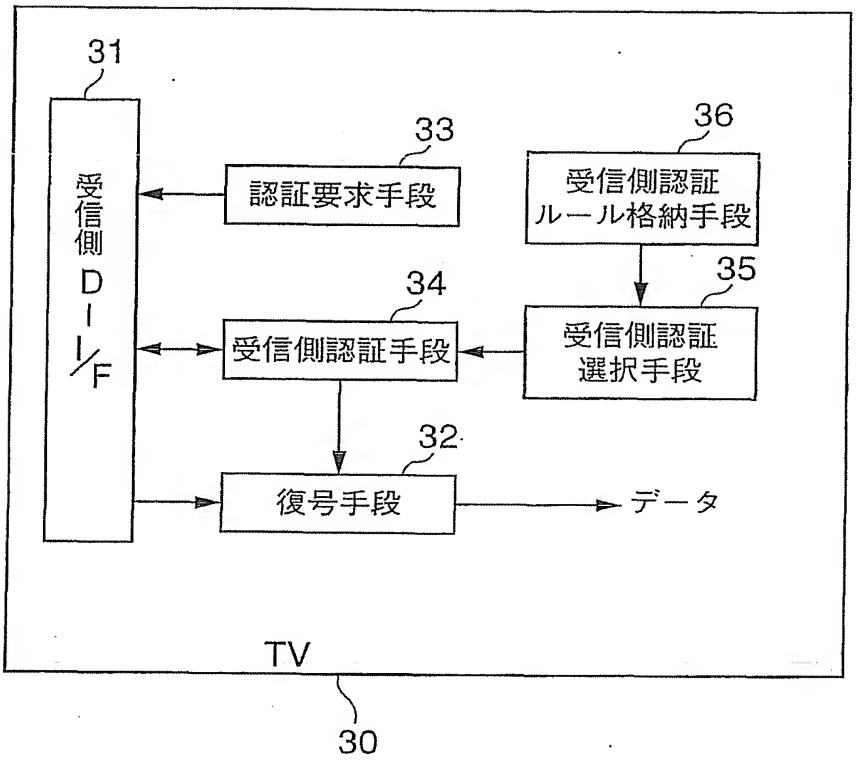
第１図


1
3
ソース
8
シンク4
4
シンク0
7
シンク3
5
シンク1
6
シンク2
(ブリッジ装置)
11
シンク7
9
シンク5
10
シンク6
2

第２図


27
デバイス情報
格納手段
26
カウント調整・
判定手段
25
認証上限数
格納手段
21
29
24
送信側認証
ルール格納手段
認証数
カウント手段
送信側
D-I/F
28
23
送信側認証
選択手段
送信側認証手段
22
データ
暗号化手段
STB
20

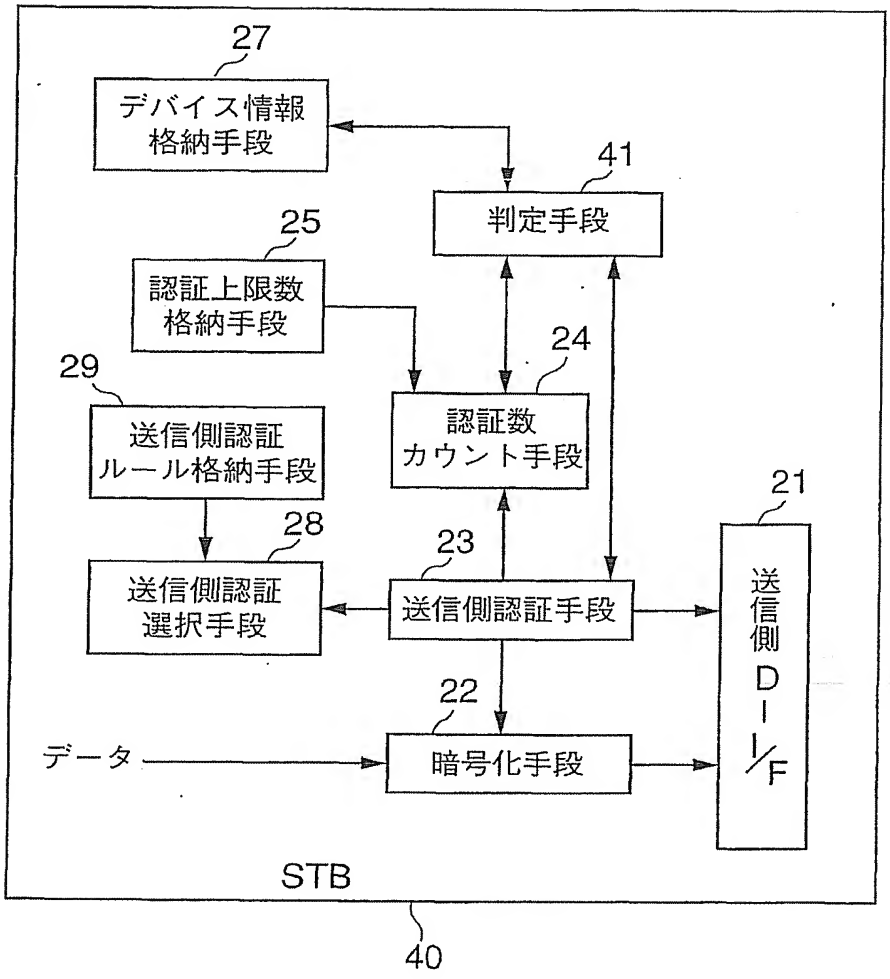
第３図


31
受信側D-I/F
33
認証要求手段
36
受信側認証ルール格納手段
35
34
受信側認証手段
受信側認証選択手段
32
復号手段
データ
TV
30

第４図

認証要求した機器	認証の種類	認証の結果	カウントしている認証数	格納しているデバイスID
なし	———	———	0	なし
シンク1(5)	認証	成功	1	シンク1(5)
シンク0(4)	認証	成功	2	シンク1(5), シンク0(4)
シンク3(7)	認証	成功	3	シンク1(5), シンク0(4), シンク3(7)
シンク4(8)	認証	拒絶	3	シンク1(5), シンク0(4), シンク3(7)
シンク0(4)	認証	成功	3	シンク1(5), シンク0(4), シンク3(7)
シンク1(5)	デクレメント認証	成功	2	シンク0(4), シンク3(7)
シンク4(8)	認証	成功	3	シンク0(4), シンク3(7), シンク4(8)

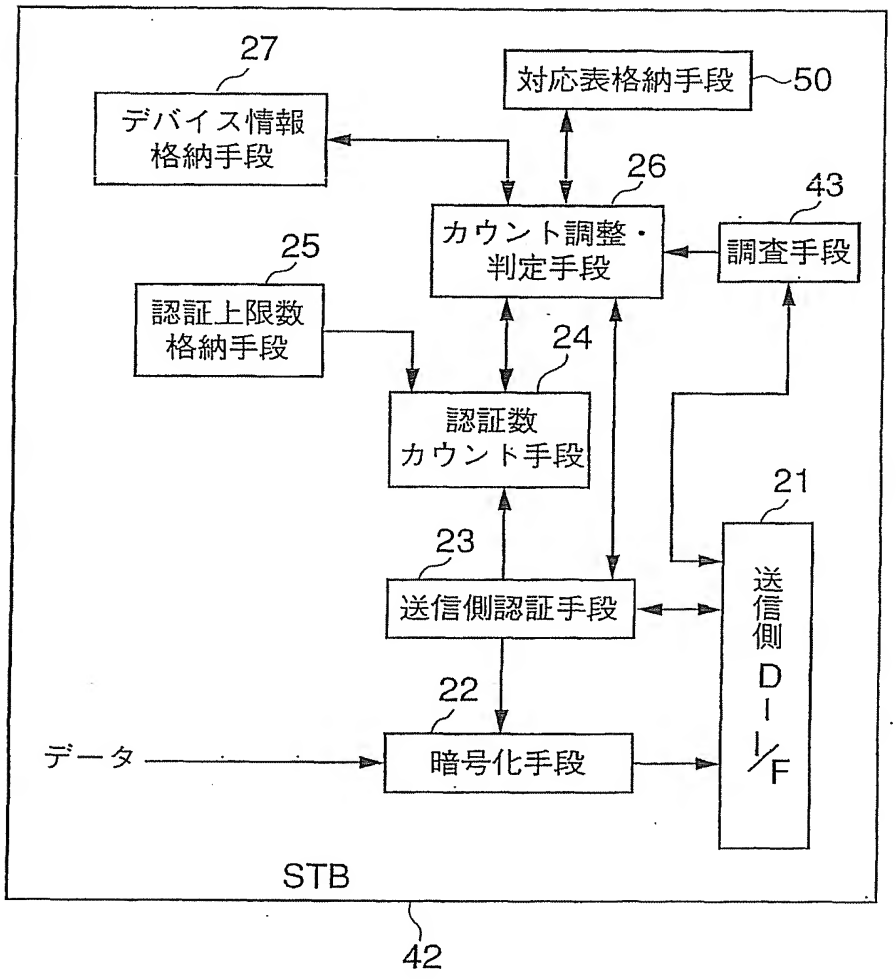
第 5 図


27
デバイス情報
格納手段
41
判定手段
25
認証上限数
格納手段
24
29
送信側認証
ルール格納手段
認証数
カウント手段
21
28
23
送信側認証
選択手段
送信側認証手段
送信側DI/F
22
データ
暗号化手段
STB
40

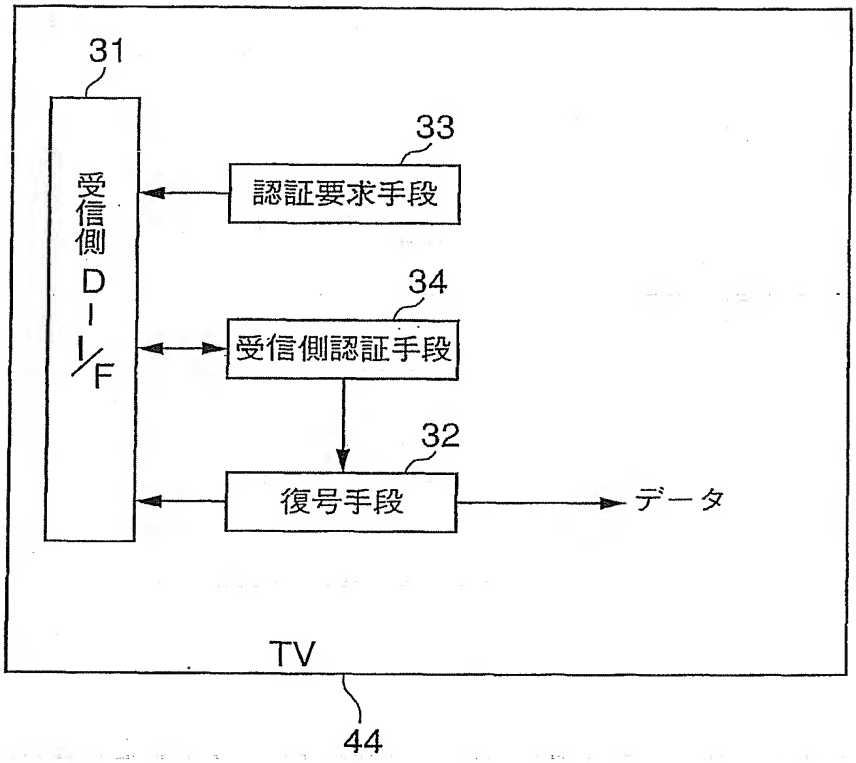
第 6 図

認証要求した機器	認証の種類	認証の結果	カウントしている認証数	格納しているデバイスID
			0	なし
シンク1(5)	認証	成功	1	シンク1(5)
シンク0(4)	認証	成功	2	シンク1(5), シンク0(4)
シンク3(7)	認証	成功	3	シンク1(5), シンク0(4), シンク3(7)
シンク4(8)	認証	拒絶	3	シンク1(5), シンク0(4), シンク3(7)
シンク1(5)	デクレメント認証	成功	2	シンク0(4), シンク3(7)
シンク4(8)	認証	成功	3	シンク0(4), シンク3(7), シンク4(8)

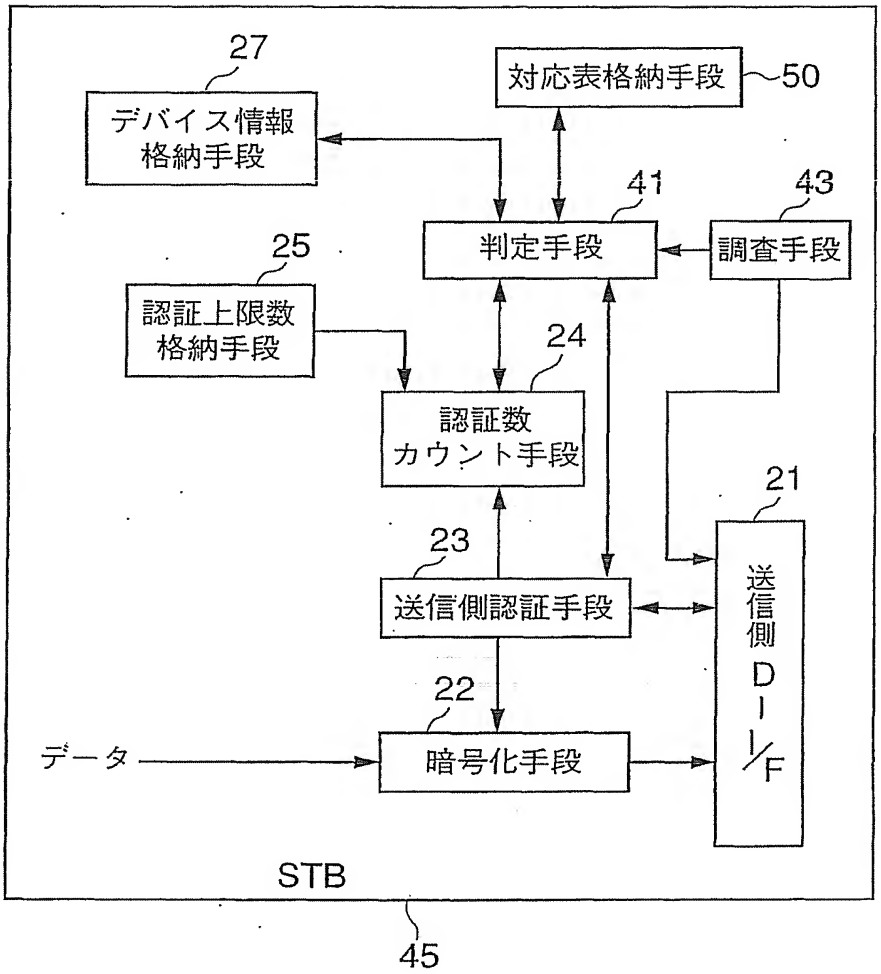
第７図


27
デバイス情報格納手段
対応表格納手段
50
26
43
カウント調整・判定手段
調査手段
25
認証上限数格納手段
24
認証数カウント手段
21
23
送信側認証手段
送信側D-I/F
22
データ
暗号化手段
STB
42

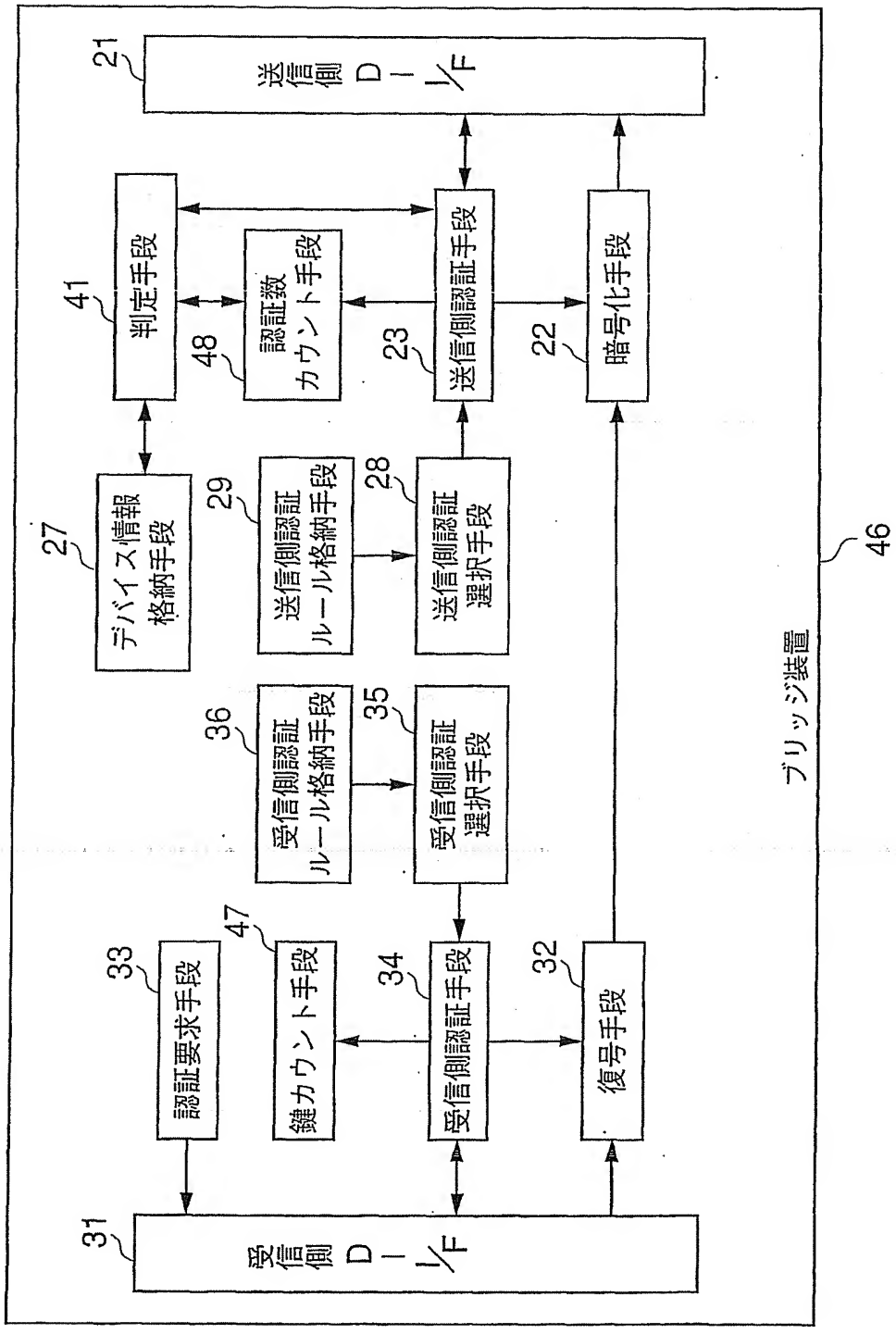
第８図



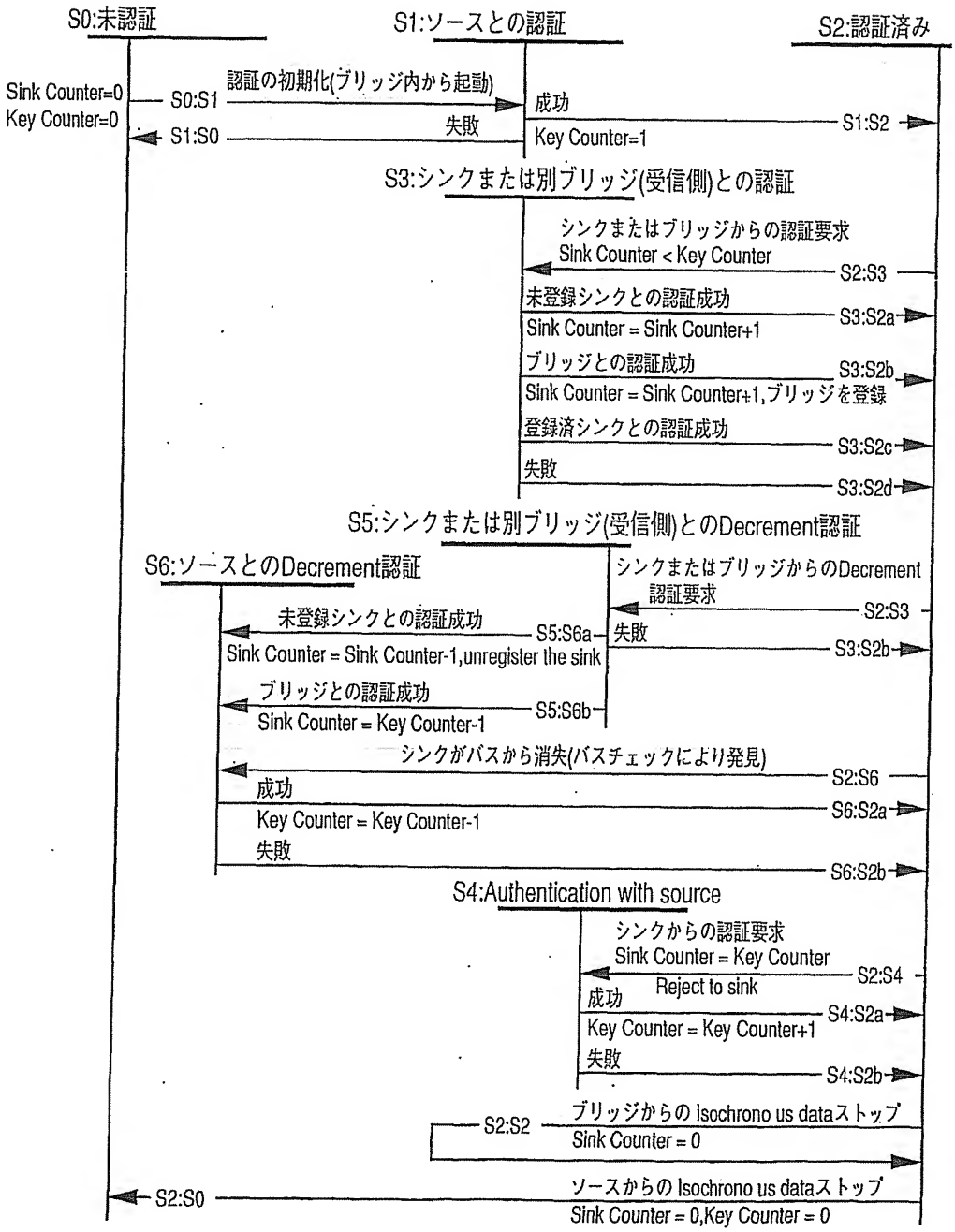
第 9 図


27
デバイス情報
格納手段
対応表格納手段
50
41
43
判定手段
調査手段
25
認証上限数
格納手段
24
認証数
カウント手段
21
23
送信側認証手段
送信側
D
I
/
F
22
データ
暗号化手段
STB
45

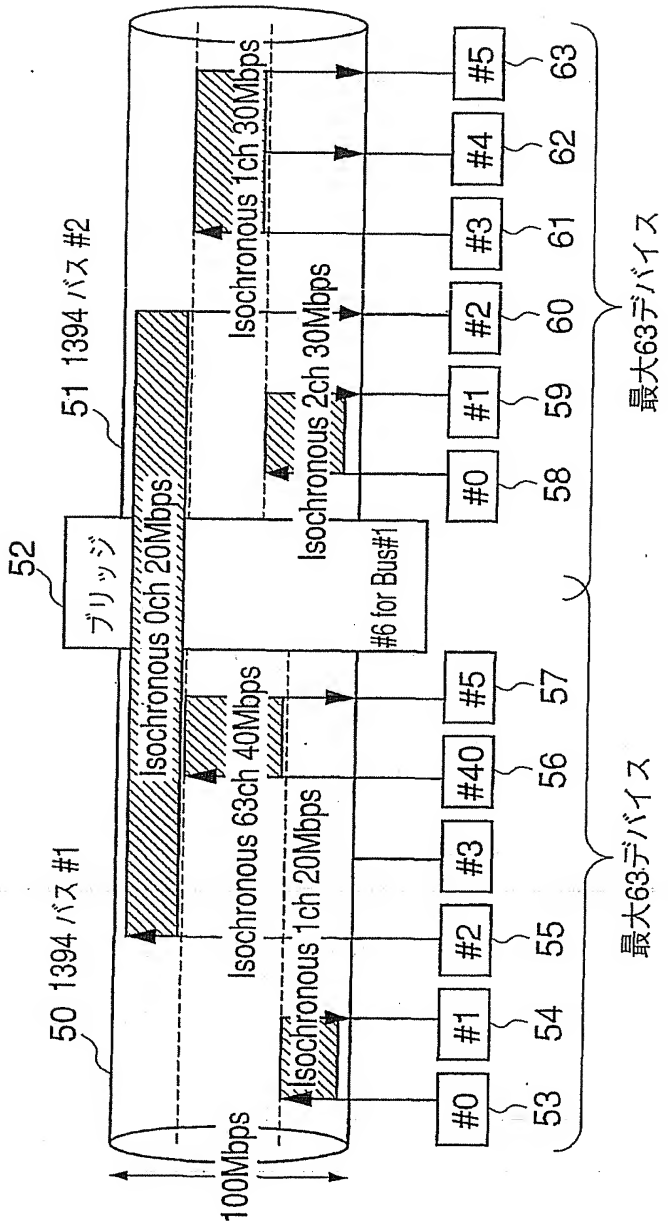
第１０図


ブリッジ装置
46
送信側 D－I／F
21
判定手段
41
認証数カウント手段
48
送信側認証手段
23
暗号化手段
22
デバイス情報格納手段
27
送信側認証ルール格納手段
29
送信側認証選択手段
28
受信側認証ルール格納手段
36
受信側認証選択手段
35
認証要求手段
33
鍵カウント手段
47
受信側認証手段
34
復号手段
32
受信側 D－I／F
31

第１１図


S0:未認証
S1:ソースとの認証
S2:認証済み
Sink Counter=0
Key Counter=0
S0:S1
認証の初期化(ブリッジ内から起動)
成功
S1:S2
失敗
S1:S0
Key Counter=1
S3:シンクまたは別ブリッジ(受信側)との認証
シンクまたはブリッジからの認証要求
Sink Counter < Key Counter
S2:S3
未登録シンクとの認証成功
S3:S2a
Sink Counter = Sink Counter+1
ブリッジとの認証成功
S3:S2b
Sink Counter = Sink Counter+1,ブリッジを登録
登録済シンクとの認証成功
S3:S2c
失敗
S3:S2d
S5:シンクまたは別ブリッジ(受信側)とのDecrement認証
S6:ソースとのDecrement認証
シンクまたはブリッジからのDecrement認証要求
S2:S3
未登録シンクとの認証成功
S5:S6a
失敗
S3:S2b
Sink Counter = Sink Counter-1,unregister the sink
ブリッジとの認証成功
S5:S6b
Sink Counter = Key Counter-1
シンクがバスから消失(バスチェックにより発見)
S2:S6
成功
S6:S2a
Key Counter = Key Counter-1
失敗
S6:S2b
S4:Authentication with source
シンクからの認証要求
Sink Counter = Key Counter
S2:S4
Reject to sink
成功
S4:S2a
Key Counter = Key Counter+1
失敗
S4:S2b
S2:S2
ブリッジからの Isochrono us dataストップ
Sink Counter = 0
S2:S0
ソースからの Isochrono us dataストップ
Sink Counter = 0,Key Counter = 0

第12図


50 1394 バス #1
51 1394 バス #2
52
ブリッジ
100Mbps
Isochronous 0ch 20Mbps
Isochronous 63ch 40Mbps
Isochronous 1ch 20Mbps
Isochronous 1ch 30Mbps
Isochronous 2ch 30Mbps
#6 for Bus#1
#0
#1
#2
#3
#40
#5
#4
#5
53
54
55
56
57
58
59
60
61
62
63
最大63デバイス
最大63デバイス